Guida per l'utente di Lenovo XClarity Administrator

Versione 4.0.0

Prima edizione (Febbraio 2023)

Contenuto

Tabelle

Riepilogo delle modifiche

Le versioni successive del software di gestione Lenovo XClarity Administrator supportano nuovi miglioramenti hardware e software, con l'aggiunta di nuove correzioni.

Per informazioni sulle correzioni, fare riferimento al file di cronologia modifiche (*.chg) fornito nel pacchetto di aggiornamento.

Questa versione supporta i seguenti miglioramenti del software di gestione.

Per informazioni sulle modifiche nelle release precedenti, vedere Novità nella documentazione online di XClarity Administrator.

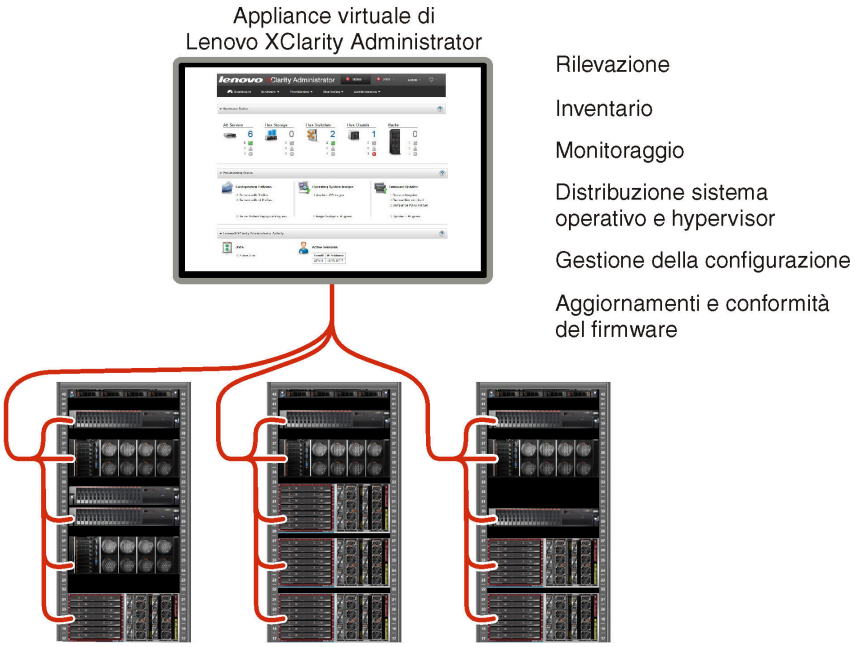
Funzione	Descrizione
Amministrazione	È possibile eseguire il push del nome FQDN (Fully-Qualified Domain Name) e delle informazioni DNS del server di gestione XClarity Administrator ai server gestiti con IMM2, XCC e XCC2, in modo che i server gestiti possano trovare il server di gestione utilizzando queste informazioni (vedere Configurazione dell'accesso alla rete).
Monitoraggio	È possibile visualizzare i dati di inventario aggiuntivi per i componenti PMEM (Persistent Memory) (vedere Visualizzazione dei dettagli di un server gestito). È possibile visualizzare i dati di inventario aggiuntivi per i dispositivi di storage (vedere Visualizzazione dei dettagli di un server gestito).
Gestione dei dispositivi	È possibile visualizzare e configurare la modalità di sicurezza per server specifici separati da XClarity Administrator (Configurazione delle impostazioni di sicurezza per un server gestito e Configurazione delle impostazioni di crittografia sul server di gestione). Gli indirizzi IP secondari sono supportati per il controller di gestione della scheda di base nei server ThinkSystem applicabili (vedere Visualizzazione dei dettagli di un server gestito).
Aggiornamenti firmware	È possibile aggiornare il firmware su tutte le librerie nastro IBM TS4300 (vedere Aggiornamento del firmware sui dispositivi gestiti).
Distribuzione del sistema operativo	È possibile distribuire i seguenti sistemi operativi nei server gestiti (vedere Sistemi operativi supportati). • Client Microsoft Windows 10 21H2, 10 22H2 e 11 22H2 • RedHat Enterprise Linux 9.x • Server Ubuntu 22.04.x

Capitolo 1. Panoramica di Lenovo XClarity Administrator

Lenovo XClarity Administrator è una soluzione centralizzata, per la gestione delle risorse, che semplifica la gestione dell'infrastruttura, velocizza i tempi di risposta e ottimizza la disponibilità dei sistemi e delle soluzioni per i server Lenovo®. Viene eseguita come un'appliance virtuale in grado di automatizzare il rilevamento, l'inventario, la tracciatura, il monitoraggio e il provisioning per server, rete e hardware di storage in un ambiente sicuro.

Ulteriori informazioni:

- XClarity Administrator: gestire l'hardware come il software
- XClarity Administrator: panoramica



XClarity Administrator dispone di un'interfaccia centrale che permette di eseguire le seguenti funzioni per tutti i dispositivi gestiti.

Gestione dell'hardware

XClarity Administrator consente una gestione dell'hardware senza agente. È in grado di rilevare automaticamente i dispositivi gestibili, inclusi il server, la rete e l'hardware di storage. La raccolta di dati dell'inventario per i dispositivi gestiti permette di disporre di un colpo d'occhio immediato dell'inventario dell'hardware gestito e del relativo stato.

Esistono varie attività di gestione per ogni dispositivo supportato, tra cui visualizzazione di stato e proprietà, configurazione di sistema e impostazioni di rete, avvio delle interfacce di gestione, accensione e spegnimento e controllo remoto. Per ulteriori informazioni sulla gestione di dispositivi, vedere Gestione dello chassis, Gestione dei server e Gestione degli switch.

Suggerimento: server, rete e hardware di storage che possono essere gestiti da XClarity Administrator vengono definiti *dispositivi*. Gli elementi hardware gestiti da XClarity Administrator vengono definiti *dispositivi gestiti*.

È possibile utilizzare la vista rack in XClarity Administrator per raggruppare i dispositivi gestiti in modo da riprodurre la configurazione del rack fisico nel data center. Per ulteriori informazioni sui rack, vedere Gestione dei rack.

Ulteriori informazioni:

- XClarity Administrator: rilevamento
- XClarity Administrator: inventario
- XClarity Administrator: controllo remoto

Monitoraggio dell'hardware

XClarity Administrator offre una vista centralizzata di tutti gli eventi e gli avvisi generati dai dispositivi gestiti. Un evento o un avviso viene passato a XClarity Administrator e visualizzato nel log eventi o nel log avvisi. Un riepilogo di tutti gli eventi e gli avvisi è visibile dal Dashboard e dalla barra di stato. Gli eventi e gli avvisi per un dispositivo specifico sono disponibili nella pagina dei dettagli di avvisi ed eventi per tale dispositivo.

Per ulteriori informazioni sul monitoraggio dell'hardware, vedere Utilizzo degli eventi e Gestione degli avvisi.

Ulteriori informazioni: XClarity Administrator: monitoraggio

Gestione della configurazione

È possibile eseguire rapidamente il provisioning e il pre-provisioning di tutti i server utilizzando una configurazione coerente. Le impostazioni di configurazione (come storage locale, adattatori I/O, impostazioni di avvio, firmware, porte, controller di gestione e impostazioni UEFI) vengono salvate come pattern server che è possibile applicare a uno o più server gestiti. Una volta aggiornati i pattern server, le modifiche vengono distribuite automaticamente ai server applicati.

I pattern server integrano inoltre il supporto per la virtualizzazione degli indirizzi I/O, pertanto è possibile virtualizzare le connessioni fabric Flex System oppure reimpiegare i server senza interruzione ne fabric.

Per ulteriori informazioni sulla configurazione dei server, vedere Configurazione dei server mediante i pattern di configurazione.

Ulteriori informazioni:

- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: pattern di configurazione

Aggiornamenti e conformità del firmware

La gestione del firmware è semplificata dall'assegnazione di criteri di conformità del firmware ai dispositivi gestiti. Una volta creato e assegnato un criterio di conformità ai dispositivi gestiti, XClarity Administrator monitora le modifiche apportate all'inventario per tali dispositivi e contrassegna i dispositivi non conformi.

Quando un dispositivo non è conforme, è possibile utilizzare XClarity Administrator per applicare e attivare gli aggiornamenti firmware per tutti i dispositivi nel suddetto dispositivo da un repository di aggiornamenti firmware gestiti.

Nota: L'aggiornamento del repository e il download di aggiornamenti firmware richiedono una connessione Internet. Se XClarity Administrator non dispone di una connessione Internet, è possibile importare manualmente gli aggiornamenti firmware nel repository.

Per ulteriori informazioni sull'aggiornamento del firmware, vedere Aggiornamento del firmware sui dispositivi gestiti.

Ulteriori informazioni:

- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: aggiornamenti firmware
- XClarity Administrator: provisioning degli aggiornamenti di sicurezza del firmware

Distribuzione del sistema operativo

È possibile utilizzare XClarity Administrator per gestire un repository di immagini del sistema operativo e per distribuire immagini del sistema operativo a un massimo di 28 server gestiti contemporaneamente.

Per ulteriori informazioni sulla distribuzione di sistemi operativi, vedere Installazione dei sistemi operativi sui server bare metal.

Ulteriori informazioni:

- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: distribuzione del sistema operativo

Gestione utenti

XClarity Administrator offre un server di autenticazione centralizzato per creare e gestire gli account utente e gestire e autenticare le credenziali degli utenti. Il server di autenticazione viene creato automaticamente quando si avvia il server di gestione per la prima volta. Gli account utente creati per XClarity Administrator possono essere utilizzati anche per eseguire il login ai server e allo chassis gestiti in modalità di autenticazione gestita. Per ulteriori informazioni sugli utenti, vedere Gestione degli account utente.

XClarity Administrator supporta tre tipi di server di autenticazione:

- **Server di autenticazione locale**. Per impostazione predefinita, XClarity Administrator è configurato in modo da utilizzare il server di autenticazione locale che si trova sul nodo di gestione.
- **Server LDAP esterno**. Attualmente, è supportato solo Microsoft Active Directory. Questo server deve trovarsi in un server Microsoft Windows esterno connesso alla rete di gestione.Quando viene utilizzato un server LDAP esterno, il server di autenticazione locale è disabilitato.
- **provider di identità SAML 2.0 esterno**. Attualmente, è supportato solo Microsoft Active Directory Federation Services (AD FS). Oltre all'immissione di un nome utente e una password, l'autenticazione a più fattori può essere configurata in modo da garantire un'ulteriore protezione attraverso la richiesta di un codice PIN, la lettura di una smart card e un certificato client.

Per ulteriori informazioni sui tipi di autenticazione, vedere Gestione del server di autenticazione.

Quando si crea un account utente, si assegna un gruppo di ruoli predefinito o personalizzato all'account utente per controllare il livello di accesso di tale utente. Per ulteriori informazioni sui gruppi di ruoli, vedere Creazione di un gruppo di ruoli personalizzato.

XClarity Administrator include un log di controllo che fornisce un record cronologico degli interventi dell'utente, come il login, la creazione di nuovi utenti o la modifica delle password utente. Per ulteriori informazioni sul log di controllo, vedere Utilizzo degli eventi.

Autenticazione dispositivo

XClarity Administrator utilizza i seguenti metodi per l'autenticazione con i server e gli chassis gestiti.

- **Autenticazione gestita**. Quando l'autenticazione gestita è abilitata, gli account utente creati in XClarity Administrator vengono utilizzati per autenticare i server e gli chassis gestiti.

  Per ulteriori informazioni sugli utenti, vedere Gestione degli account utente.
- **Autenticazione locale**. Quando l'autenticazione gestita è disabilitata, le credenziali memorizzate definite in XClarity Administrator vengono utilizzate per autenticare i server gestiti. Le credenziali memorizzate devono corrispondere a un account utente attivo sul dispositivo o in Active Directory.

Per ulteriori informazioni sulle credenziali memorizzate, vedere Gestione delle credenziali memorizzate.

Protezione

Se l'ambiente deve essere conforme agli standard NIST SP 800-131A, XClarity Administrator consente di disporre di un ambiente completamente conforme.

XClarity Administrator supporta certificati SSL autofirmati (emessi da un'autorità di certificazione interna) e certificati SSL esterni (emessi da un'autorità di certificazione privata o commerciale).

I firewall su chassis e server possono essere configurati per accettare richieste in entrata solo da XClarity Administrator.

Per ulteriori informazioni sulla protezione, vedere Implementazione di un ambiente sicuro.

Assistenza e supporto

XClarity Administrator può essere configurato in modo da raccogliere e inviare file di diagnostica automaticamente al fornitore di servizi preferito quando si verificano determinati eventi che richiedono assistenza in XClarity Administrator e nei dispositivi gestiti. È possibile scegliere di inviare i file di diagnostica al Supporto Lenovo utilizzando Call Home o a un altro fornitore di servizi utilizzando SFTP. È inoltre possibile raccogliere manualmente i file di diagnostica, aprire un record del problema e inviare i file di diagnostica al Centro assistenza clienti Lenovo.

Ulteriori informazioni:  XClarity Administrator: assistenza e supporto

Automatizzazione delle attività con gli script

XClarity Administrator può essere integrato in piattaforme di automazione e gestione esterne di livello superiore tramite API REST aperte. Utilizzando le API REST, XClarity Administrator può integrarsi facilmente con l'infrastruttura di gestione esistente.

Il toolkit PowerShell fornisce una libreria di cmdlet per l'automatizzazione del provisioning e la gestione delle risorse da una sessione di Microsoft PowerShell. Il toolkit Python fornisce una libreria di API e comandi basata su Python per automatizzare il provisioning e la gestione delle risorse da un ambiente OpenStack, come Ansible o Puppet. Entrambi i toolkit forniscono un'interfaccia per le API REST di XClarity Administrator che consente di automatizzare funzioni come:

- Login a XClarity Administrator
- Gestione e annullamento della gestione di chassis, server, dispositivi di storage e switch TOR (Top-of-Rack) (dispositivi)
- Raccolta e visualizzazione di dati di inventario per dispositivi e componenti
- Distribuzione di un'immagine del sistema operativo in uno o più server
- Configurazione di server attraverso l'utilizzo di pattern di configurazione
- Applicazione di aggiornamenti firmware ai dispositivi

Integrazione con un altro software gestito

I moduli XClarity Administrator integrano XClarity Administrator con il software di gestione di terze parti per fornire funzioni di rilevamento, monitoraggio, configurazione e gestione che consentono di ridurre il costo e la complessità dell'amministrazione ordinaria del sistema per i dispositivi supportati.

Per ulteriori informazioni su XClarity Administrator, vedere i documenti seguenti:
- Lenovo XClarity Integrator per Microsoft System Center
- Lenovo XClarity Integrator per VMware vCenter

Per ulteriori considerazioni, vedere Considerazioni sulla gestione nella documentazione online di XClarity Administrator.

Ulteriori informazioni:

- Panoramica di Lenovo XClarity Integrator per Microsoft System Center
- Lenovo XClarity Integrator per VMware vCenter

Documentazione

La XClarity Administrator documentazione online viene regolarmente aggiornata in inglese. Vedere Documentazione online di XClarity Administrator per le informazioni e le procedure più recenti.

La documentazione online è disponibile nelle seguenti lingue:

- Tedesco (de)
- Inglese (en)
- Spagnolo (es)
- Francese (fr)
- Italiano (it)
- Giapponese (ja)
- Coreano (ko)
- Portoghese brasiliano (pt_BR)
- Russo (ru)
- Tailandese (th)
- Cinese semplificato (zh_CN)
- Cinese tradizionale (zh_TW)

È possibile modificare la lingua della documentazione online nei seguenti modi:

- Modificare l'impostazione della lingua nel browser Web
- Aggiungere `?lang=`*<language_code>* alla fine dell'URL, ad esempio, per visualizzare la documentazione online in cinese semplificato:
  `http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html`**?lang=zh_CN**

Login a XClarity Administrator

Eseguire il login all'interfaccia Web di Lenovo XClarity Administrator utilizzando un browser Web supportato.

Prima di iniziare

Accertarsi di utilizzare uno dei seguenti browser Web supportati:

- Chrome™ 48.0 o versioni successive (55.0 o versioni successive per la console remota)
- Firefox® ESR 38.6.0 o versioni successive
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 o versioni successive (IOS7 o versioni successive e OS X)

Nota: l'avvio delle interfacce del controller di gestione da XClarity Administrator mediante il browser Web Safari non è supportato.

Assicurarsi di eseguire il login all'interfaccia Web di XClarity Administrator da un sistema con connettività di rete al nodo di gestione di XClarity Administrator.

Procedura

Per eseguire il login all'interfaccia Web di XClarity Administrator, attenersi alla procedura descritta di seguito.

Passo 1. Puntare il browser all'indirizzo IP di XClarity Administrator.

> **Suggerimento:** l'accesso all'interfaccia Web avviene attraverso una connessione sicura. Accertarsi di utilizzare **https**.

- **Per i contenitori**. Utilizzare l'indirizzo IPv4 specificato per la variabile ${ADDRESS} per accedere a XClarity Administrator utilizzando il seguente URL:
  `https://<IPv4_address>/ui/login.html`

  Ad esempio:
  `https://192.0.2.10/ui/login.html`

- **Per le appliance virtuali**. L'indirizzo IP utilizzato dipende dalla modalità di configurazione dell'ambiente.

  se le reti Eth0 e Eth1 si trovano in sottoreti diverse, e in entrambe viene usato DHCP, utilizzare l'indirizzo IP *Eth1* per accedere all'interfaccia Web ed eseguire la configurazione iniziale. Al primo avvio di XClarity Administrator sia Eth0 che Eth1 ottengono un indirizzo IP assegnato da DHCP mentre il gateway predefinito di XClarity Administrator viene impostato sul gateway assegnato da DHCP per *Eth1*.

  Utilizzo di un indirizzo IPv4 statico
  Se è stato specificato un indirizzo IPv4 in eth0_config, utilizzare tale indirizzo IPv4 per accedere a XClarity Administrator mediante il seguente URL:
  `https://<IPv4_address>/ui/login.html`

  Ad esempio:
  `https://192.0.2.10/ui/login.html`

  Utilizzo di un server DHCP nello stesso dominio di broadcast di XClarity Administrator
  Se un server DHCP è configurato nello stesso dominio di broadcast di XClarity Administrator, utilizzare l'indirizzo IPv4 visualizzato nella console della macchina virtuale di XClarity Administrator per accedere a XClarity Administrator mediante il seguente URL:
  `https://<IPv4_address>/ui/login.html`

  Ad esempio:
  `https://192.0.2.10/ui/login.html`

  Utilizzo di un server DHCP in un dominio di broadcast differente da XClarity Administrator
  Se un server DHCP *non* è configurato nello stesso dominio di broadcast, utilizzare l'indirizzo IPv6 locale rispetto al collegamento (Link-Local Address, LLA) visualizzato per eEth0, la rete di gestione, nella console della macchina virtuale di XClarity Administrator per accedere a XClarity Administrator, ad esempio:

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

  Suggerimento: l'indirizzo IPv6 locale rispetto al collegamento (LLA) viene ricavato dall'indirizzo MAC dell'interfaccia.

Attenzione: se la configurazione di XClarity Administrator viene eseguita in remoto, è necessario disporre della connettività alla stessa rete di livello 2. L'accesso deve essere eseguito da un indirizzo non instradato fino al completamento della configurazione iniziale. Pertanto, è consigliabile eseguire l'accesso a XClarity Administrator da un'altra macchina virtuale che disponga della connettività a XClarity Administrator. Ad esempio, è possibile accedere a XClarity Administrator da un'altra macchina virtuale sull'host in cui è installato XClarity Administrator.

- **Firefox:**

  Per accedere all'interfaccia Web di XClarity Administrator da un browser Firefox, eseguire il login utilizzando il seguente URL. Quando si immettono gli indirizzi IPv6, è necessario inserire le parentesi quadre.

  `https://[<IPv6_LLA>/ui/login.html]`

  Ad esempio, rispetto all'esempio precedente relativo a Eth0, immettere il seguente URL nel browser Web:

  `https://[fe80:21a:64ff:fe12:3456]/ui/login.html`

- **Internet Explorer:**

  Per accedere all'interfaccia Web di XClarity Administrator da un browser Internet Explorer, eseguire il login utilizzando il seguente URL. Quando si immettono gli indirizzi IPv6, è necessario inserire le parentesi quadre.

  `https://[<IPv6_LLA>%25<zone_index>]/ui/login.html`

  dove *<zone_index>* è l'identificativo dell'adattatore Ethernet connesso alla rete di gestione dal computer su cui si è avviato il browser Web. Se si utilizza un browser in Windows, usare il comando `ipconfig` per trovare l'indice di area, visualizzato dopo il segno di percentuale (%) nel campo **Indirizzo IPv6 locale rispetto al collegamento** per l'adattatore. Nell'esempio seguente l'indice di area è "30."

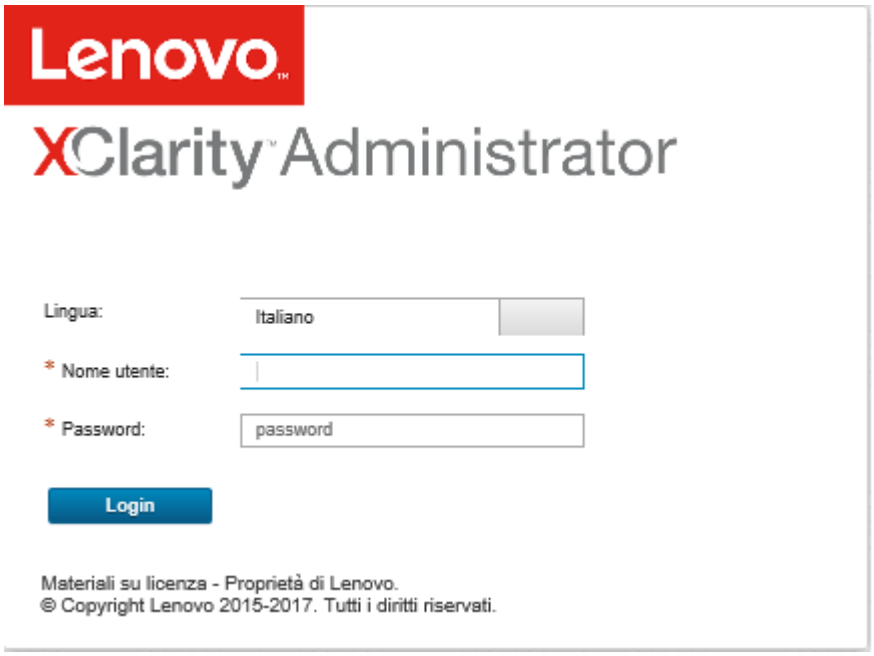
  ```
  PS C:> ipconfig
  Configurazione IP Windows

  Adattatore Ethernet vEthernet (teamVirtualSwitch):

     Suffisso DNS specifico della connessione  . :
     Indirizzo IPv6 locale del collegamento . . . . . : 2001:db8:56ff:fe80:bea3%30
     Configurazione automatica dell'indirizzo IPv4. . : 192.0.2.30
     Gateway predefinito . . . . . :
  ```

  Se si utilizza un browser su Linux, utilizzare il comando `ifconfig` per trovare l'indice di area. Anche il nome dell'adattatore (generalmente Eth0) può essere utilizzato come indice di area.

  Ad esempio, rispetto agli esempi precedenti relativi a Eth0 e all'indice di area, immettere il seguente URL nel browser Web:

  `https://[2001:db8:56ff:fe80:bea3%2530]/ui/login.html`

Verrà visualizzata la pagina di login iniziale di XClarity Administrator:



Passo 2. Selezionare la lingua desiderata dall'elenco a discesa **Lingua**.

Nota: i valori e le impostazioni di configurazione forniti dai dispositivi gestiti potrebbero essere disponibili solo in inglese.

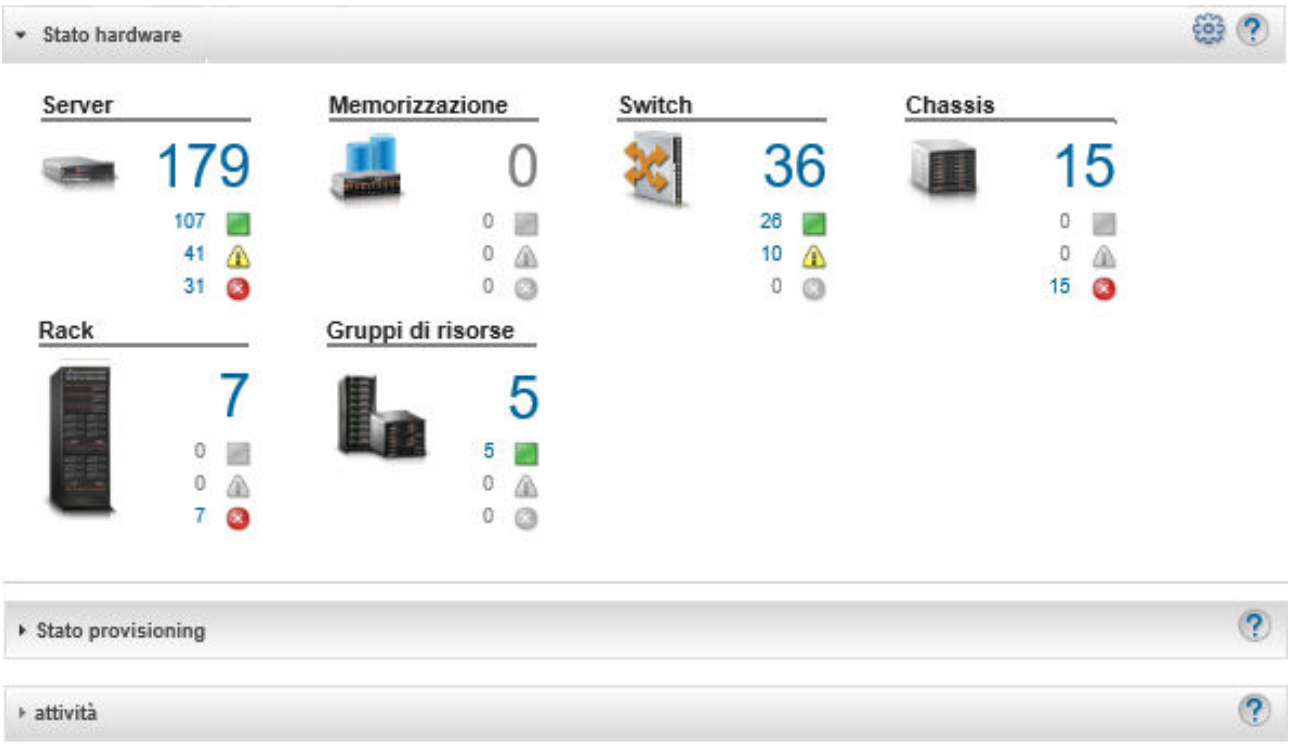
Passo 3. Immettere un ID utente e una password validi e fare clic su **Login**.

La prima volta che si esegue il login con un account utente, verrà richiesto di modificare la password. Le password devono rispondere ai seguenti criteri:

- (1) Deve contenere almeno un carattere alfabetico e non deve avere più di due caratteri sequenziali, tra cui sequenze di caratteri alfabetici, cifre e tasti della tastiera QWERTY (ad esempio, "abc", "123" e "asd" non sono consentiti).
- (2) Deve contenere almeno un numero (0-9).
- (3) Deve contenere almeno *due* dei caratteri che seguono.
  - Caratteri alfabetici maiuscoli (A - Z)
  - Caratteri alfabetici minuscoli (a - z)
  - Caratteri speciali ; @ _ ! ' $ & +
- (4) Non deve essere una ripetizione né l'inversione del nome utente.
- (5) Non deve contenere consecutivamente più di due degli stessi caratteri (ad esempio, "aaa", "111" e "..." non sono ammessi).

Al termine

Verrà visualizzata la pagina Dashboard di XClarity Administrator:



Nota: se il sistema operativo host si arresta in modo imprevisto, è possibile che, al momento del login a XClarity Administrator, venga visualizzato un messaggio di errore di autenticazione. Per risolvere questo problema, ripristinare XClarity Administrator dall'ultimo backup per accedere al server di gestione (vedere Backup di Lenovo XClarity Administrator).

È possibile eseguire le seguenti azioni dal menu azioni utente (ADMIN_USER) sulla barra del titolo di XClarity Administrator.

- È possibile consultare le informazioni su come utilizzare XClarity Administrator nel sistema di guida integrato, facendo clic su **Guida**.

  La XClarity Administrator documentazione online viene regolarmente aggiornata in inglese. Vedere Documentazione online di XClarity Administrator per le informazioni e le procedure più recenti.
- È possibile visualizzare la licenza di XClarity Administrator facendo clic su **Licenza**.
- È possibile visualizzare le informazioni sulla versione di XClarity Administrator facendo clic su **Informazioni su**.
- È possibile modificare la lingua dell'interfaccia utente facendo clic su **Modifica lingua**.
- È possibile effettuare il logout dalla sessione corrente facendo clic su **Disconnetti**.
- È possibile inviare idee o fornire feedback su XClarity Administrator facendo clic su **Invia idee** o **Invia feedback**.
- È possibile porre domande e individuare risposte sul Sito Web del forum della community dedicata a Lenovo XClarity facendo clic su **Visita forum**.

Suggerimenti e tecniche dell'interfaccia utente

Tenere presente questi suggerimenti e queste tecniche durante l'utilizzo dell'interfaccia utente di Lenovo XClarity Administrator

Visualizzazione di più o meno dati per pagina

È possibile cambiare il numero di righe che vengono visualizzate su ogni pagina utilizzando i collegamenti nella parte inferiore destra della tabella. È possibile visualizzare **10**, **25**, **50** o **tutte** le righe

Ricerca di dati in elenchi di grandi dimensioni

La maggior parte dei campi può accettare fino a 128 caratteri.

Sono disponibili diversi modi per visualizzare un sottoinsieme di un elenco di grandi dimensioni in base a criteri specifici.

- È possibile ordinare le righe della tabella facendo clic sull'intestazione di colonna.

  La modifica dell'ordinamento della colonna di una tabella è permanente nelle sessioni utente.
- È possibile utilizzare le icone **Filtra per** e l'elenco a discesa **Mostra** disponibile in alcune pagine per visualizzare un sottoinsieme di dati basati sui criteri selezionati.
- È possibile perfezionare ulteriormente il sottoinsieme immettendo del testo (ad esempio, un nome o un indirizzo IP) nel campo **Filtra** per individuare i dati presenti in qualsiasi colonna disponibile.

  È possibile scegliere dalle ultime 10 ricerche selezionando le ricerche dal menu a discesa nel campo **Filtri**. L'ultima ricerca attiva su una pagina è permanente nelle sessioni utente.

Visualizzazione dei dati delle colonne

Se le dimensioni delle colonne impediscono la visualizzazione di tutte le informazioni nella cella della tabella (indicata dai puntini di sospensione), è possibile visualizzare le informazioni complete in un popup passando il mouse sul testo nella cella.

Configurazione delle colonne delle tabelle

È possibile configurare le tabelle per visualizzare le informazioni importanti per l'utente.

- È possibile scegliere le colonne da visualizzare o da nascondere facendo clic su **Tutte le azioni → Attiva/Disattiva colonne**.
- È possibile riordinare le colonne trascinando le intestazioni delle colonne nella posizione preferita.

Modifica della lingua dell'interfaccia utente

Al primo login è disponibile un'opzione per impostare la lingua dell'interfaccia utente.

Dopo aver eseguito il login, è possibile modificare la lingua dell'interfaccia utente facendo clic sul menu azioni utente (

) e quindi selezionare **Modifica lingua**. Selezionare la lingua che si desidera visualizzare.

Nota: Il sistema di guida viene visualizzato nella stessa lingua impostata per l'interfaccia utente.

Richiesta di supporto

XClarity Orchestrator offre diversi modi per ottenere assistenza per l'interfaccia utente.

- Alcune pagine forniscono dettagli aggiuntivi su uno specifico campo o stato mediante le icone **Guida** (). Passare il cursore sull'icona per visualizzare un popup con informazioni utili.
- Per ottenere informazioni su come eseguire azioni specifiche dall'interfaccia utente, fare clic sul menu azioni utente (

) e quindi selezionare **Guida**

Utilizzo dell'app Lenovo XClarity Mobile

Lenovo XClarity Administrator offre un'app per dispositivi mobili Android e iOS. È possibile utilizzare l'app Lenovo XClarity Mobile per monitorare in modo sicuro i sistemi fisici, ottenere notifiche e avvisi di stato in tempo reale, nonché per intraprendere azioni su attività di livello comune per i sistemi. L'applicazione può anche connettersi direttamente tramite una porta USB abilitata a un server ThinkSystem e fornire la funzionalità LCD virtuale.

Ulteriori informazioni:  Panoramica di Lenovo XClarity Mobile

Tramite l'applicazione XClarity Mobile, è possibile completare le seguenti attività:
- Configurare le impostazioni di rete e le proprietà
- Visualizzare il riepilogo dello stato di ciascun dispositivo XClarity Administratorcollegato.
- Visualizzare il riepilogo dello stato di tutti i dispositivi gestiti.
- Visualizzare le viste grafiche (mappe) di chassis, server rack e dispositivi di storage.
- Visualizzare i gruppi di risorse definiti in XClarity Administrator.
- Visualizzare le informazioni sulle porte dello switch rack e modificare lo stato delle porte configurate.
- Monitorare l'inventario e lo stato dettagliato di ogni dispositivo gestito.
- Monitorare eventi di controllo, eventi di gestione e hardware, avvisi e processi.
- Accendere o spegnere il LED di posizione di un dispositivo gestito.
- Accendere, spegnere, riavviare o riposizionare un dispositivo gestito.
- Avviare la raccolta dei dati diagnostici.
- Visualizzare lo stato e le informazioni sulla garanzia del dispositivo
- Configurare la funzione di notifica automatica dei problemi tramite Call Home.
- Visualizzare il riepilogo dei ticket di assistenza aperti e cancellare ticket di assistenza.
- Inviare notifiche eventi ai dispositivi mobili (vedere Inoltro di eventi a dispositivi mobili).
- Visualizzare il riepilogo degli utenti attivi e l'utilizzo delle risorse di sistema.
- Inviare feedback su questa applicazione mobile al supporto Lenovo.
- Collegare il dispositivo mobile direttamente a un server ThinkSystem per gestire il server mediante l'applicazione XClarity Mobile (per dispositivi che supportano il tethering USB).
- Scaricare i dati di servizio di Lenovo XClarity Controller quando il dispositivo mobile è collegato a un server ThinkSystem.

È anche possibile collegare il dispositivo mobile direttamente ai server ThinkSystem, quindi avviare l'app XClarity Mobile ed eseguire il login al controller di gestione della scheda di base del server utilizzando le stesse credenziali Web e CLI. È disponibile un menu di azioni e informazioni aggiuntive che include:

- Servizio
  - Condividere le informazioni di riepilogo mediante e-mail o altri mezzi forniti dal dispositivo mobile.
  - Cancellare i log eventi e il log di controllo.
  - Eseguire il download del log eventi e del log di controllo sullo storage locale del dispositivo mobile oppure trasmettere il log con qualsiasi mezzo fornito dal dispositivo mobile.
  - Eseguire il download del file di servizio BMC FFDC sullo storage locale del dispositivo mobile oppure trasmettere il file con qualsiasi mezzo fornito dal dispositivo mobile.
  - Visualizzare i dati del grafico cronologico su alimentazione, temperature e utilizzo del sistema
  - Abilitare la modalità di servizio "One-Touch", che fornisce un riepilogo immediato di avvisi attivi e informazioni critiche sul dispositivo.
- Installazione e configurazione iniziale
  - Gestire un nuovo dispositivo utilizzando il XClarity Administrator selezionato.
  - Configurare le proprietà del server, quali la posizione e le informazioni di contatto per la configurazione iniziale.
  - Visualizzare e modificare le impostazioni dell'interfaccia di rete BMC IPv4 e IPv6.
  - Specificare l'ordine di avvio e le impostazioni di avvio singolo.
  - Modificare l'assegnazione della porta USB del pannello anteriore.
  - Visualizzare il numero di riavvii del server e le ore totali di alimentazione.

- Azioni di alimentazione
  - Accendere e spegnere il server, riavviare il server o attivare NMI.
  - Reimpostare BMC.

Suggerimento: una volta avviata l'applicazione, è necessario aggiornarla per visualizzare lo stato, l'inventario, gli eventi e i processi aggiornati.

Prerequisiti

- I tablet iOS sono supportati solo con la risoluzione dello schermo di iPhone. I tablet Android attualmente non sono supportati.
- Sono supportati i seguenti sistemi operativi mobili:
  - Android 7-11
  - iOS 10 e versioni successive

    Nota:

    - Android 5 è supportato solo per XClarity Mobile 2.3.0 e versioni precedenti.
    - Il riconoscimento facciale utilizzato sui dispositivi iPhone X/XR/XS non è supportato.
- Verificare che sia disponibile una connessione di rete da dispositivo mobile a istanze XClarity Administrator. Ciò potrebbe richiedere l'uso di una soluzione VPN. Consultare l'amministratore di rete per richiedere assistenza.
- Importare il certificato CA per ogni istanza XClarity Administrator.

  Importante: Tutte le connessioni a XClarity Administrator utilizzano il protocollo HTTPS. Tuttavia, affinché la connessione venga considerata attendibile e che i dati possano essere inviati ai dispositivi mobili, deve essere disponibile una catena di certificati valida. Per creare una catena di certificati attendibili, è necessario importare l'autorità di certificazione autofirmata di XClarity Administrator nel dispositivo mobile.

  Per importare il certificato CA autofirmato per *ogni istanza di XClarity Administrator* nel dispositivo mobile, completare le seguenti operazioni.

  1. Scaricare il certificato CA in un sistema locale:
     a. Collegarsi all'istanza di XClarity Administrator utilizzando un browser Web sul sistema locale.
     b. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Sicurezza** per visualizzare la pagina Sicurezza.
     c. Fare clic su **Autorità di certificazione** nella sezione Gestione certificati. Verrà visualizzata la pagina Autorità di certificazione.
     d. Fare clic su **Scarica certificato radice autorità di certificazione**.

        Attenzione: Generalmente, non è necessario fare clic su **Rigenera certificato radice autorità di certificazione** per completare questo processo. Così facendo, si potrebbe interrompere la comunicazione con i dispositivi gestiti, tranne se non viene seguita la procedura corretta. Per ulteriori informazioni, vedere Utilizzo dei certificati di sicurezza.
     e. Fare clic su **Salva come DER** o **Salva come PEM** per salvare il file del certificato CA in formato DER o PEM sul sistema locale. Il formato PEM funziona nella maggior parte dei casi.
  2. Trasferire il file del certificato CA sul dispositivo mobile utilizzando, ad esempio, un repository di storage accessibile (come Dropbox™), l'e-mail o il trasferimento di file tramite cavo.
  3. Importare il certificato CA attendibile:
     - (Android) Generalmente, per completare questa procedura è necessario selezionare **Impostazioni → Sicurezza → Installa** dallo storage del telefono e quindi il file del certificato scaricato.

Importante: Se il certificato CA correttamente installato non è firmato da terze parti, sui dispositivi Android viene visualizzato il messaggio `La rete può essere monitorata da terze parti sconosciute.` Poiché il certificato CA viene generato in un ambiente sicuro, questo messaggio può essere ignorato. Prima di ignorare il messaggio, verificare che si riferisca al certificato CA di XClarity Administrator.

– (iOS) Avviare il client e-mail sul dispositivo mobile e fare clic sul collegamento del documento per importare il certificato CA attendibile.

Attenzione: Per iOS 10.3 e versioni successive, i certificati importati non sono considerati attendibili per impostazione predefinita. Per confermare l'attendibilità dei certificati, selezionare **Impostazioni → Generale → Informazioni su → Impostazioni attendibilità certificati**, quindi abilitare l'attendibilità dei certificati.

Installazione e configurazione

1. Scaricare l'applicazione XClarity Mobile da iTunes App Store (iOS) o Google Play Store (Android).
2. Per installare l'applicazione, seguire le istruzioni sul dispositivo mobile.

   Importante: Per sbloccare la schermata di accesso e utilizzare l'applicazione XClarity Mobile è necessario un codice di sicurezza di livello sistema operativo mobile. Se il codice di sicurezza non è impostato è necessario configurarlo durante l'installazione.
3. Fare clic su **Impostazioni** per aggiungere o modificare le connessioni a più istanze di XClarity Administrator utilizzando il rilevamento automatico o fornendo un indirizzo IP e le credenziali utente, impostando un codice PIN per l'applicazione, modificando le impostazioni del log di controllo e degli eventi e selezionando la lingua preferita.

Collegamento diretto ai server ThinkSystem

I server Lenovo ThinkSystem includono una porta USB sul pannello anteriore che può essere utilizzata per collegare il dispositivo mobile e abilitare funzionalità simili a quelle disponibili sul pannello del display LCD delle informazioni sul sistema su altri server Lenovo.

Per gestire un server ThinkSystem mediante collegamento diretto al server, completare le seguenti operazioni.

1. Commutare l'USB del pannello anteriore del server in BMC effettuando una delle operazioni indicate di seguito.
   a. Dal controller di gestione CLI, eseguire il comando `usbfp`
   b. Dall'interfaccia Web del controller di gestione fare clic su **Configurazione BMC → Rete → Gestione porta USB del pannello anteriore**.
   c. Tenere premuto il LED di posizione ID blu sul pannello anteriore per almeno 3 secondi finché la luce non lampeggia ogni due secondi.
2. Collegare il cavo USB del telefono alla porta USB sul pannello anteriore del server ThinkSystem.
3. Abilitare il tethering USB sul dispositivo mobile.
   a. Per iOS, fare clic su **Impostazioni → Cellulare → Hotspot personale**.
   b. Per Android, fare clic su **Impostazioni → Hotspot mobile e tethering → Tethering USB**.
4. Sul dispositivo mobile, avviare l'app XClarity Mobile.
5. Se il rilevamento automatico è disabilitato, fare clic su **Rilevamento** sulla pagina Rilevamento USB per collegare il controller di gestione del server e raccogliere informazioni su inventario, stato, firmware e configurazione di rete, oltre a un elenco degli eventi attivi più recenti.

Suggerimento:

- Accertarsi di utilizzare un cavo USB di alta qualità in grado di supportare dati e alimentazione. Tenere presente che alcuni cavi forniti con i dispositivi mobili sono solo a scopo di ricarica.

Nota: Per eseguire il collegamento a ThinkSystem SD530, è necessario utilizzare un cavo da micro USB a USB o un adattatore di alta qualità.

- Il server USB collegato deve essere acceso per affinché le statistiche complete di tensione, temperatura e utilizzo vengano riportate nelle schede riepilogative dello stato.
- Se i server USB collegati non dispongono di un pulsante/LED di identificazione blu sul pannello anteriore, è necessario utilizzare l'interfaccia Web del controller di gestione o l'interfaccia CLI per modificare la selezione per la gestione della porta USB sul pannello anteriore, se necessario.
- Le modifiche apportate dall'interfaccia di rete del controller di gestione dall'app XClarity Mobile vengono applicate immediatamente, senza richiedere il riavvio del controller di gestione. Ad esempio, se l'interfaccia IPv4 viene modificata da un indirizzo statico in DHCP, l'interfaccia ottiene immediatamente un indirizzo DHCP assegnato.
- Nella scheda NewsFeed, la scheda degli eventi attivi più recenti visualizza inizialmente fino a tre eventi attivi elencati nella scheda Eventi attivi del controller di gestione. Sull'app mobile, se si tocca la scheda, vengono visualizzati tutti gli eventi attivi. Tenere presente che si tratta di un elenco di eventi attivi e risolti, e non di un elenco completo degli eventi.

Utilizzo della modalità dimostrativa

È possibile abilitare la **Modalità dimostrativa** nella pagina "Impostazioni" per popolare l'applicazione XClarity Mobile con i dati dimostrativi di due istanze XClarity Administrator, inclusi rack e chassis. In questa modalità, è possibile visualizzare il riepilogo di stato delle istanze di XClarity Administrator, visualizzare lo stato dettagliato e l'inventario dei dispositivi, nonché monitorare eventi e avvisi. Tuttavia, le azioni di gestione, come accensione e spegnimento, non sono supportate.

Nota:

- È possibile abilitare la modalità dimostrativa solo quando non sono attive connessioni alle istanze effettive di XClarity Administrator.
- Quando la modalità dimostrativa è abilitata, non è possibile aggiungere connessioni alle istanze effettive di XClarity Administrator.

Ricerca

È possibile utilizzare il campo **Cerca** per visualizzare i dispositivi gestiti con un nome o uno stato specifico (Critico, Avvertenza o Normale). Ad esempio, se si cerca "crit," vengono visualizzati solo i dispositivi gestiti in stato critico con i nomi che includono "crit".

Risoluzione dei problemi

Problemi di installazione:

- L'app per dispositivi mobili Android è firmata con una chiave sicura per aumentare la sicurezza. La dimensione della chiave sicura è stata aumentata nella nuova versione. Poiché l'applicazione con firma non corrisponde alla firma dell'app precedente, il processo di installazione di sicurezza di Android impedisce l'aggiornamento automatico.

  Per aggiornare l'app per dispositivi mobili, disinstallare la versione corrente dell'app, scaricare la versione più recente dell'app Android dal negozio delle app e reinstallare l'app. Nella maggior parte dei dispositivi Android, l'app può essere disinstallata utilizzando la voce di menu **Impostazioni → Applicazioni → Gestione applicazioni**.

Problemi di connettività:

- La funzione di tethering USB in iOS 14, 14.0.1 e 14.0.2 non funziona correttamente e, pertanto, la funzione di tethering dell'app Lenovo XClarity Mobile non è disponibile per queste versioni di iOS. Ciò incide solo sulla gestione del palmare collegato all'USB nel data center, non incide sulla gestione remota mediante i dispositivi mobili che supportano le comunicazioni cellulari e Wi-Fi. La gestione remota può essere

utilizzata per collegare e raccogliere dati da XClarity Administratore per eseguire azioni di gestione sui dispositivi gestiti.

Se è necessaria la funzione di gestione del palmare collegato all'USB, non eseguire l'aggiornamento a iOS 14.

Questa notifica verrà aggiornata quando Apple risolverà il problema con iOS 14.

- XClarity Mobile richiede una connessione di rete disponibile da dispositivo mobile a istanze di XClarity Administrator. Ciò potrebbe richiedere l'uso di una soluzione VPN. Consultare l'amministratore di rete per richiedere assistenza.
- Le connessioni da dispositivo mobile a ogni istanza di XClarity Administrator richiedono una catena di certificati attendibili. Consultare la documentazione online per istruzioni su download e installazione dei certificati CA attendibili su dispositivi mobili.

  Se il certificato CA installato correttamente non è firmato da terze parti, viene visualizzato il messaggio `La rete può essere monitorata da terze parti sconosciute`. Poiché il certificato CA viene generato in un ambiente sicuro, questo messaggio può essere ignorato. Prima di ignorare il messaggio, verificare che si riferisca al certificato CA di XClarity Administrator.
- Quando si sposta il dispositivo mobile da una rete VPN (Virtual Private Network) a una rete locale o viceversa, potrebbe essere visualizzato il messaggio `il gateway sicuro ha rifiutato il tentativo di connessione. È necessario un nuovo tentativo di connessione allo stesso o ad altri gateway sicuri, che richiede la riautenticazione`. Accedere a Lenovo XClarity Mobile per continuare a utilizzare l'applicazione.

Problemi di sicurezza:

- Se si dimentica il codice PIN, disinstallare e reinstallare l'applicazione XClarity Mobile. Quindi, ristabilire tutte le connessioni.
- Se si cancellano le credenziali dal dispositivo Android, la chiave di crittografia viene eliminata. È necessario ristabilire tutte le connessioni.

Problemi relativi agli eventi:

- Per impostazione predefinita, il log eventi mostra gli eventi di gestione e hardware ricevuti nelle ultime 24 ore, mentre il log di controllo mostra gli eventi di controllo ricevuti nelle ultime 2 ore. Se durante i periodi di tempo selezionati non si riceve alcun evento, il log eventi e il log di controllo non vengono visualizzati nella pagina "Monitoraggio" di XClarity Mobile.
- Se viene configurata la funzione di inoltro eventi di XClarity Administrator per inviare gli eventi a un account e-mail, i collegamenti nell'e-mail potrebbero non funzionare sui dispositivi Android. Verificare che la versione di Android e l'applicazione e-mail supportino i collegamenti ipertestuali. Se i collegamenti ipertestuali non sono sostenuti, utilizzare un'altra applicazione e-mail.

Problemi relativi al sistema di guida:

- Su alcuni dispositivi, il sistema di guida non viene adattato correttamente alle dimensioni dello schermo. Utilizzare i controlli del sistema di guida per ottimizzare e quindi ridurre la pagina.

Capitolo 2. Amministrazione di Lenovo XClarity Administrator

Diverse attività di amministrazione, come l'aggiunta di server o la visualizzazione di processi, possono essere eseguite da Lenovo XClarity Administrator.

Gestione di autenticazione e autorizzazione

Lenovo XClarity Administrator offre meccanismi di sicurezza che consentono di verificare le credenziali di un utente e di controllare l'accesso a risorse e attività.

Gestione del server di autenticazione

Per impostazione predefinita, Lenovo XClarity Administrator utilizza un server LDAP (Lightweight Directory Access Protocol) locale per autenticare le credenziali utenti.

Informazioni su questa attività

Server di autenticazione supportati

Il *server di autenticazione* è un registro utente utilizzato per autenticare le credenziali utente. Lenovo XClarity Administrator supporta i seguenti tipi di server di autenticazione.

- **Server di autenticazione locale**. Per impostazione predefinita, XClarity Administrator è configurato per utilizzare il server LDAP (Lightweight Directory Access Protocol) che risiede nel server di gestione.
- **Server LDAP esterno**. Attualmente, solo Microsoft Active Directory e OpenLDAP sono supportati. Questo server deve trovarsi in un server Microsoft Windows esterno connesso alla rete di gestione. Quando viene utilizzato un server LDAP esterno, il server di autenticazione locale è disabilitato.

  Attenzione: Per configurare il metodo di collegamento Active Directory in modo da utilizzare le credenziali di login, il firmware del controller BMC (Baseboard Management Controller) di ciascun server gestito deve essere aggiornato a settembre 2016 o successivo.
- **Sistema di gestione delle identità esterno**. Attualmente è supportato solo CyberArk.

  Se gli account utente per un server ThinkSystem o ThinkAgile sono integrati in CyberArk, è possibile scegliere di utilizzare XClarity Administrator per recuperare le credenziali tramite CyberArk al fine di accedere al server durante la configurazione iniziale dei server per la gestione (con autenticazione gestita o locale). Prima che le credenziali possano essere recuperate da CyberArk, i percorsi CyberArk devono essere definiti in XClarity Administrator e l'attendibilità reciproca deve essere stabilita tra CyberArk e XClarity Administrator utilizzando l'autenticazione TLS reciproca tramite i certificati client.
- **SAML esterno provider di identità**. Attualmente, è supportato solo Microsoft Active Directory Federation Services (AD FS). Oltre all'immissione di un nome utente e una password, l'autenticazione a più fattori può essere configurata in modo da garantire un'ulteriore protezione attraverso la richiesta di un codice PIN, la lettura di una smart card e un certificato client. Quando viene utilizzato un provider di identità SAML, il server di autenticazione locale non viene disabilitato. Gli account utente locali sono richiesti per accedere direttamente a uno chassis gestito o al server (tranne se Incapsulamento non è abilitato su tale dispositivo), per l'autenticazione PowerShell e API REST, nonché per il ripristino se l'autenticazione esterna non è disponibile.

  È possibile scegliere di utilizzare sia un server LDAP esterno che un provider di identità esterno. Se entrambi sono abilitati, il server LDAP esterna viene utilizzato per accedere direttamente ai dispositivi da gestire, mentre il provider di identità viene utilizzato per accedere al server di gestione.

Autenticazione dispositivo

Per impostazione predefinita, i dispositivi vengono gestiti utilizzando l'autenticazione gestita di XClarity Administrator per eseguire il login ai dispositivi. Quando si gestiscono i server rack e lo chassis Lenovo, è possibile scegliere di utilizzare l'autenticazione locale o gestita per eseguire il login ai dispositivi.

- Quando l'*autenticazione locale* viene utilizzata per i server rack, lo chassis Lenovo e gli switch rack Lenovo, XClarity Administrator utilizza una credenziale memorizzata per eseguire l'autenticazione al dispositivo. La *credenziale memorizzata* può essere un account utente attivo sul dispositivo o un account utente in un server Active Directory.

  Prima di gestire il dispositivo utilizzando l'autenticazione locale è necessario creare le credenziali memorizzate in XClarity Administrator che corrispondono a un account utente attivo sul dispositivo o un account utente in un server Active Directory (vedere Gestione delle credenziali memorizzate nella documentazione online di XClarity Administrator).

  Nota:

  – I dispositivi RackSwitch supportano solo le credenziali memorizzate per l'autenticazione. Le credenziali utente di XClarity Administrator non sono supportate.
- L'*autenticazione gestita* consente di gestire e monitorare più dispositivi utilizzando le credenziali del server di autenticazione XClarity Administrator invece delle credenziali locali. Quando l'autenticazione gestita viene utilizzata per un dispositivo (diverso dai server ThinkServer e System x M4 o dagli switch), XClarity Administrator configura il dispositivo gestito e i relativi componenti installati per utilizzare il server di autenticazione XClarity Administrator per la gestione centralizzata.
  – Quando è abilitata l'autenticazione gestita, è possibile gestire i dispositivi utilizzando le credenziali memorizzate o inserite manualmente (vedere Gestione degli account utente e nella documentazione online di XClarity Administrator).

    La credenziale memorizzata viene utilizzata solo finché XClarity Administrator non configura le impostazioni LDAP sul dispositivo. Successivamente, eventuali modifiche delle credenziali memorizzate non incidono sulla gestione o sul monitoraggio di tale dispositivo.

    Nota: Quando è abilitata l'autenticazione gestita per un dispositivo, non è possibile modificare le credenziali memorizzate per tale dispositivo utilizzando XClarity Administrator.
  – Se viene utilizzato un server LDAP esterno o locale come server di autenticazione XClarity Administrator, gli account utente definiti nel server di autenticazione vengono utilizzati per eseguire il login a XClarity Administrator, CMM e controller di gestione della scheda di base nel dominio di XClarity Administrator. Gli account utente del controller di gestione e CMM locali sono disabilitati.
  – Se viene utilizzato un provider di identità SAML 2.0 come server di autenticazione XClarity Administrator, gli account SAML non saranno accessibili per i dispositivi gestiti. Tuttavia quando si utilizzano un provider di identità SAML e un server LDAP insieme, se il provider di identità utilizza gli account esistenti nel server LDAP, gli account utente LDAP possono essere utilizzati per eseguire il login ai dispositivi gestiti mentre i metodi di autenticazione più avanzati forniti da SAML 2.0 (come autenticazione a più fattori e Single Sign-On) possono essere utilizzati per eseguire il login a XClarity Administrator.
  – La funzione Single Sign-On consente a un utente già connesso a XClarity Administrator di eseguire automaticamente il login al controllo di gestione della scheda di base. L'opzione Single Sign-On è abilitata per impostazione predefinita quando un server ThinkSystem o ThinkAgile viene inserito nella gestione da XClarity Administrator (a meno che il server non sia gestito con password CyberArk). È possibile configurare l'impostazione globale per abilitare o disabilitare la funzione Single Sign-On per tutti i server ThinkSystem e ThinkAgile gestiti. L'abilitazione dell'opzione Single Sign-On per un server ThinkSystem o ThinkAgile specifico ha la precedenza sull'impostazione globale per tutti i server ThinkSystem e ThinkAgile (vedere).

    Nota: Single Sign-On viene disabilitato automaticamente quando si utilizza il sistema di gestione delle identità CyberArk per l'autenticazione.

- Quando l'autenticazione gestita è abilitata per i server ThinkSystem SR635 e SR655:
  - Il firmware del controller di gestione della scheda di base supporta fino a cinque ruoli utente LDAP. XClarity Administrator aggiunge questi ruoli utente LDAP ai server durante la gestione: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** e **lxc-os-admin**.

    È necessario assegnare gli utenti ad almeno uno dei ruoli utente LDAP specificati per comunicare con i server ThinkSystem SR635 e SR655.
  - Il firmware del controller di gestione non supporta gli utenti LDAP con lo stesso nome utente locale del server.
- Per i server ThinkServer e System x M4, il server di autenticazione XClarity Administrator non viene utilizzato. Di contro, viene creato un account IPMI sul dispositivo con il prefisso "LXCA_", seguito da una stringa casuale. (Gli account utente IPMI locali esistenti non vengono disabilitati). Quando si annulla la gestione di un server ThinkServer, l'account utente "LXCA_" viene disabilitato e il prefisso "LXCA_" viene sostituito con il prefisso "DISABLED_". Per determinare se un server ThinkServer è gestito da un'altra istanza, XClarity Administrator verifica gli account IPMI con il prefisso "LXCA_". Se si sceglie di forzare la gestione di un server ThinkServer gestito, tutti gli account IPMI del dispositivo con il prefisso "LXCA_" vengono disabilitati e rinominati. Valutare la possibilità di cancellare manualmente gli account IPMI non più in uso.

  Se si utilizzano credenziali inserite manualmente, XClarity Administrator crea automaticamente una credenziale memorizzata e la utilizza per gestire il dispositivo.

  Nota: Quando è abilitata l'autenticazione gestita per un dispositivo, non è possibile modificare le credenziali memorizzate per tale dispositivo utilizzando XClarity Administrator.
  - Ogni volta che si gestisce un dispositivo utilizzando le credenziali inserite manualmente, viene creata una nuova credenziale memorizzata per tale dispositivo, anche se è stata creata un'altra credenziale memorizzata per il dispositivo durante un processo di gestione precedente.
  - Quando si annulla la gestione di un dispositivo, XClarity Administrator non elimina le credenziali memorizzate create automaticamente per tale dispositivo durante il processo di gestione.

Account di ripristino

Se si specifica una password di ripristino, XClarity Administrator disabilita l'account utente CMM locale o del controller di gestione e crea un nuovo account utente di ripristino (`RECOVERY_ID`) sul dispositivo per l'autenticazione futura. Se il server di gestione non funziona, è possibile utilizzare l'account `RECOVERY_ID` per eseguire il login al dispositivo e ripristinare le funzioni di gestione degli account del dispositivo, finché il nodo di gestione non viene ripristinato o sostituito.

Se si annulla la gestione di un dispositivo che dispone di un account utente `RECOVERY_ID`, tutti gli account utente locali vengono abilitati e l'account `RECOVERY_ID` viene eliminato.

- Se si modificano gli account utente locali disabilitati (ad esempio, se si modifica una password), le modifiche non hanno effetto sull'account `RECOVERY_ID`. In modalità di autenticazione gestita, l'account `RECOVERY_ID` è l'unico account utente attivato e operativo.
- Utilizzare l'account `RECOVERY_ID` solo in caso di emergenza, ad esempio, se il server di gestione non funziona o se si verifica un problema alla rete che impedisce al dispositivo di comunicare con XClarity Administrator per autenticare gli utenti.
- La password `RECOVERY_ID` viene specificata quando si rileva il dispositivo. Assicurarsi di registrare la password per gli usi successivi.

Per informazioni sul recupero della gestione di un dispositivo, vedere "Ripristino della gestione con un modulo CMM dopo un errore del server di gestione" a pagina 223, "Ripristino della gestione del server tower o rack dopo un errore del server di gestione" a pagina 274.

Configurazione di un server di autenticazione LDAP esterno

È possibile scegliere di utilizzare un server di autenticazione LDAP esterna invece del server di autenticazione locale Lenovo XClarity Administrator sul nodo di gestione.

Prima di iniziare

Prima di configurare il server di autenticazione esterna, è necessario completare la configurazione iniziale di XClarity Administrator.

Sono supportati i seguenti server di autenticazione esterna:

- OpenLDAP
- Microsoft Active Directory. Deve trovarsi in un server Microsoft Windows esterno connesso alla rete di gestione, alla rete di dati o a entrambe.

Verificare che tutte le porte richieste per il server di autenticazione esterna siano aperte su rete e firewall. Per informazioni sui requisiti delle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.

È necessario creare o rinominare i gruppi di ruoli del server di autenticazione locale in modo che corrispondano ai gruppi definiti nel server di autenticazione esterna.

Verificare che nel server di autenticazione locale siano disponibili uno o più utenti con autorità **lxc-ripristino**. È possibile utilizzare questo account utente locale per autenticarsi direttamente a XClarity Administrator quando si verifica un errore di comunicazione con il server LDAP esterno.

Nota: Quando XClarity Administrator è configurato per utilizzare un server di autenticazione esterna, la pagina "Gestione utenti" dell'interfaccia Web di XClarity Administrator è disabilitata.

Attenzione: In Active Directory, per configurare il metodo di associazione in modo da utilizzare le credenziali di login, il firmware del controller di gestione della scheda di base di ciascun server gestito deve essere aggiornato a settembre 2016 o successivo.

XClarity Administrator esegue un controllo della connettività ogni 5 minuti per mantenere la connettività ai server LDAP esterni configurati. Durante questo controllo della connettività negli ambienti con molti server LDAP potrebbe verificarsi un elevato utilizzo della CPU. Per ottenere prestazioni migliori, assicurarsi che tutti i server LDAP nel dominio, o la maggior parte di essi, siano raggiungibili oppure impostare il metodo di selezione del server di autenticazione su **Usa server preconfigurati** e specificare solo i server LDAP noti e raggiungibili.

Procedura

Per configurare XClarity Administrator per utilizzare un server di autenticazione esterna, completare le seguenti operazioni.

Passo 1. Configurazione del metodo di autenticazione utente per Microsoft Active Directory o OpenLDAP.

Se si sceglie di utilizzare l'autenticazione non sicura, non è richiesta alcuna configurazione aggiuntiva. Per impostazione predefinita, i controller di dominio Windows Active Directory o OpenLDAP utilizzano l'autenticazione LDAP non sicura.

Se si sceglie di utilizzare l'autenticazione LDAP sicura, è necessario configurare i controller di dominio per consentire l'autenticazione LDAP sicura. Per ulteriori informazioni sulla configurazione delle impostazioni di autenticazione LDAP sicura in Active Directory, vedere Articolo sul certificato LDAPS (LDAP over SSL) sul sito Web Microsoft TechNet.

Per verificare che i controller di dominio Active Directory siano configurati per utilizzare l'autenticazione LDAP sicura:

- Individuare l'evento `LDAP su SSL (Secure Sockets Layer) è ora disponibile` l'evento nella finestra "Visualizzatore eventi" dei controller dominio.
- Utilizzare lo strumento di Windows `ldp.exe` per verificare la connettività LDAP sicura ai controller dominio.

Passo 2. Importare il certificato server Active Directory o OpenLDAP oppure il certificato radice dell'autorità di certificazione che ha firmato il certificato server.

a. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

b. Fare clic su **Certificati attendibili** nella sezione "Gestione certificati".

c. Fare clic sull'icona **Crea** ( ) per aggiungere un certificato.

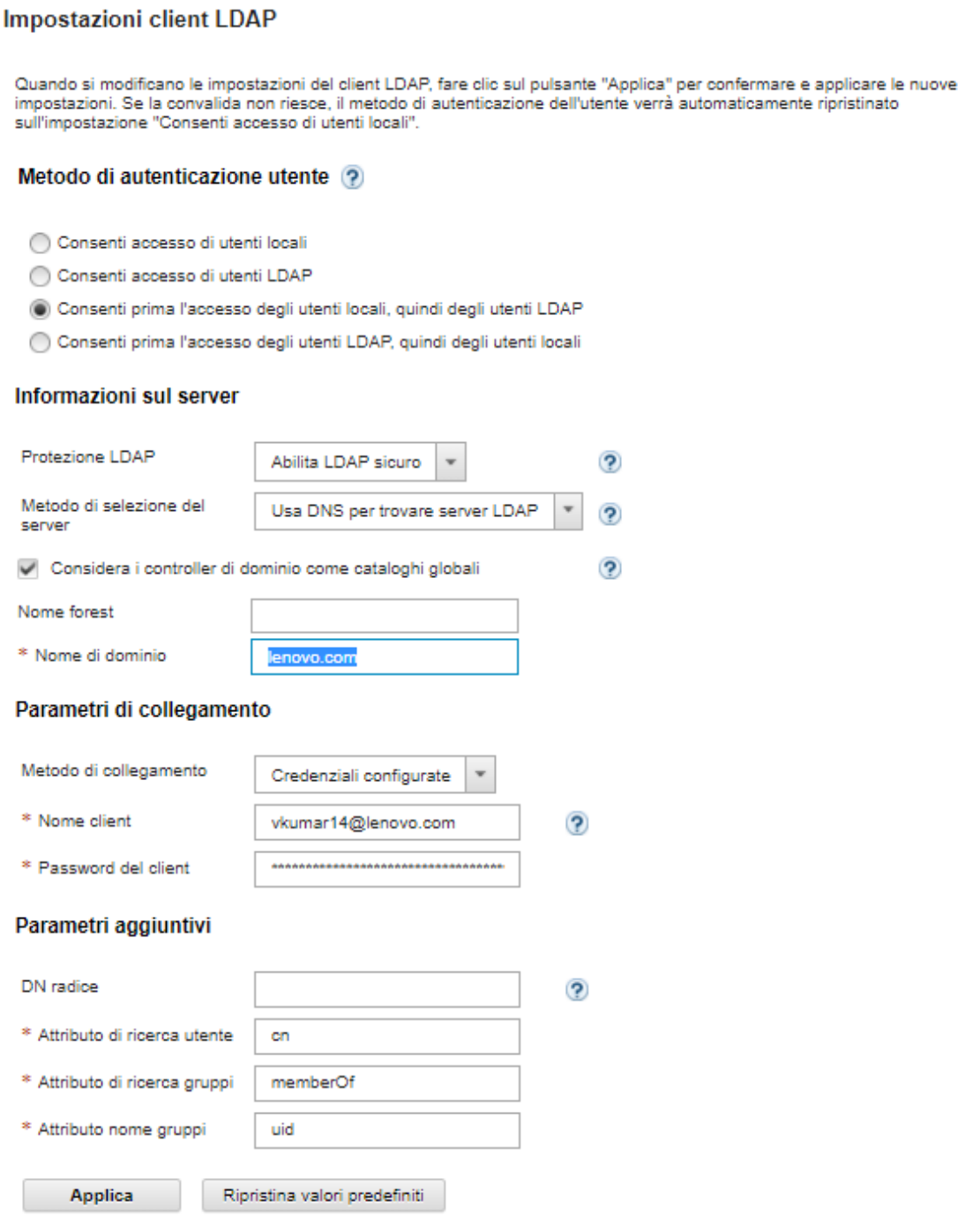
d. Individuare il file o incollare il testo del certificato con formattazione PEM.

e. Fare clic su **Crea**.

Passo 3. Configurare il client LDAP di XClarity Administrator:

a. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

b. Fare clic su **Client LDAP** nella sezione "Utenti e gruppi" per visualizzare la finestra di dialogo Impostazioni client LDAP.



c. Compilare la finestra di dialogo in base ai seguenti criteri.

1. Selezionare uno dei seguenti metodi di autenticazione utente:

   - **Consenti accesso di utenti locali**. L'autenticazione viene eseguita utilizzando l'autenticazione locale. Se questa opzione è selezionata, tutti gli account utente sono disponibili nel server di autenticazione locale sul nodo di gestione.
   - **Consenti accesso di utenti LDAP**. L'autenticazione viene eseguita da un server LDAP esterno. Questo metodo consente la gestione remota degli account utente. Quando questa opzione è selezionata, tutti gli account utente esistono in remoto su un server LDAP esterno.

- **Consenti prima l'accesso degli utenti locali, quindi degli utenti LDAP**. Il server di autenticazione locale esegue prima l'autenticazione. In caso di errore, l'autenticazione viene eseguita da un server LDAP esterno.
- **Consenti prima utenti LDAP, poi utenti locali**. Un server LDAP esterno esegue prima l'autenticazione. In caso di errore, l'autenticazione viene eseguita dal server di autenticazione locale.

2. Scegliere se abilitare o disabilitare LDAP sicuro:
   - **Abilita LDAP sicuro**. XClarity Administrator utilizza il protocollo LDAPS per collegarsi in modo sicuro al server di autenticazione esterna. Se questa opzione è selezionata, per abilitare il supporto LDAP sicuro, è necessario configurare anche i certificati attendibili.
   - **Disabilita LDAP sicuro**. XClarity Administrator utilizza un protocollo non sicuro per collegarsi al server di autenticazione esterna. Se si seleziona questa impostazione, l'hardware potrebbe essere più vulnerabile agli attacchi di sicurezza.
3. Selezionare uno dei seguenti metodi di scelta del server:
   - **Utilizza server preconfigurati**. XClarity Administrator utilizza le porte e gli indirizzi IP specificati per rilevare il server di autenticazione esterna.

     Se si seleziona questa opzione, specificare fino a quattro porte e indirizzi IP del server preconfigurati. Il client LDAP tenta di eseguire l'autenticazione utilizzando il primo indirizzo del server. Se l'autenticazione non riesce, il client LDAP tenta di eseguire l'autenticazione utilizzando l'indirizzo IP successivo.

     Se il numero di porta per una voce *non è* impostato in modo esplicito su `3268` o `3269`, la voce identifica un controller di dominio.

     Quando il numero di porta è impostato su `3268` o `3269`, la voce identifica un catalogo globale. Il client LDAP tenta di eseguire l'autenticazione utilizzando il controller di dominio per il primo indirizzo IP configurato del server. In caso di errore, il client LDAP tenta di eseguire l'autenticazione utilizzando il controller di dominio per l'indirizzo IP successivo del server.

     Importante: È necessario specificare almeno un controller di dominio, anche se il catalogo globale è specificato. Se si specifica solo il catalogo globale l'operazione viene comunque completata, ma la configurazione non è valida.

     Quando la modalità di crittografia è impostata su NIST-800-131A, XClarity Administrator potrebbe non essere in grado di collegarsi a un server LDAP esterno utilizzando una porta sicura (ad esempio, mediante LDAPS sulla porta predefinita 636) se il server LDAP non è in grado di stabilire una connessione TLS (Transport Layer Security) versione 1.2 con il client LDAP in XClarity Administrator.
   - **Usa DNS per trovare server LDAP**. XClarity Administrator utilizza il nome di dominio specificato o il nome forest per individuare dinamicamente il server di autenticazione esterna. Il nome di dominio e il nome forest vengono utilizzati per ottenere un elenco dei controller di dominio mentre il nome forest viene utilizzato per ottenere un elenco di server del catalogo globale.

     Attenzione: Quando si utilizza DNS per trovare i server LDAP, verificare che l'account utente utilizzato per eseguire l'autenticazione al server di autenticazione esterna sia in hosting sui controller di dominio specificati. Se l'account utente è in hosting su un controller di dominio secondario, includere il controller di dominio secondario nell'elenco di richieste di servizio.
4. Selezionare uno dei seguenti metodi di collegamento:

- **Credenziali configurate**. Selezionare questo metodo di collegamento per utilizzare il nome e la password del client per collegare XClarity Administrator al server di autenticazione esterna. Se il collegamento non riesce, anche il processo di autenticazione fallisce

  Il nome del client può essere qualsiasi nome supportato dal server LDAP, come nome distinto, AMAccountName, nome NetBIOS, o UserPrincipalName. Il nome del client deve essere un account utente del dominio che disponga almeno dei privilegi di sola lettura. Ad esempio:
  ```
  cn=username,cn=users,dc=example,dc=com
  domain\username
  username@domain.com
  username
  ```

  Attenzione: Se si modifica la password del client del server di autenticazione esterna, verificare che sia aggiornata anche la nuova password di XClarity Administrator . Per ulteriori informazioni, vedere Impossibile eseguire il login a XClarity Administrator nella documentazione online di XClarity Administrator.

- **Credenziali di login**. Selezionare questo metodo di associazione per utilizzare nome utente e password Active Directory o OpenLDAP per associare XClarity Administrator al server di autenticazione esterna.

  L'ID utente e la password specificati vengono utilizzati solo per verificare il collegamento al server di autenticazione. Se l'operazione riesce, le impostazioni del client LDAP vengono salvate, ma le credenziali di login di prova specificate non vengono salvate. Tutti i futuri collegamenti utilizzeranno nome utente e password utilizzati per eseguire il login a XClarity Administrator.

  Nota:

  – È necessario avere eseguito il login a XClarity Administrator utilizzando un ID utente completo (ad esempio, `administrator@domain.com` o `DOMAIN\admin`).

  – Per il metodo di collegamento è necessario utilizzare un nome completo del client di prova.

  Attenzione: Per configurare il metodo di collegamento in modo da utilizzare le credenziali di login, il firmware del controller di gestione di ciascun server gestito deve essere aggiornato a settembre 2016 o successivo.

5. Nel campo **DN radice**, si consiglia di non specificare un nome distinto radice, in particolare per ambienti con più domini. Quando questo campo è vuoto, XClarity Administrator interroga il server di autenticazione esterna per i contesti di denominazione. Se si utilizza DNS per rilevare il server di autenticazione esterna o se si specificano più server (ad esempio, `dc=example,dc=com`), è possibile specificare facoltativamente la voce iniziale della struttura di directory LDAP. In questo caso, le ricerche vengono eseguite utilizzando il nome distinto radice specificato come base della ricerca.
6. Specificare l'attributo da utilizzare per cercare il nome utente.

   Quando il metodo di collegamento è impostato su **Credenziali configurate**, il collegamento iniziale al server LDAP è seguito da una richiesta di ricerca che richiama informazioni specifiche sull'utente, come DN utente, autorizzazioni di login e appartenenza al gruppo. Questa richiesta di ricerca deve specificare il nome dell'attributo che rappresenta gli ID utente su tale server. Il nome dell'attributo è configurato in questo campo. Se questo campo è lasciato vuoto, il valore predefinito sarà **cn**.
7. Specificare il nome dell'attributo utilizzato per identificare i gruppi a cui appartiene un utente. Se questo campo viene lasciato vuoto, verrà utilizzato il valore predefinito **memberOf**.

8. Specificare il nome dell'attributo utilizzato per identificare il nome del gruppo configurato dal server LDAP. Se questo campo è vuoto, il valore predefinito è **uid**.

d. Fare clic su **Applica**.

XClarity Administrator prova a verificare la configurazione per rilevare gli errori comuni. Se il test non riesce, vengono visualizzati i messaggi di errore che indicano l'origine degli errori. Se il test riesce e le connessioni ai server specificati vengono completate correttamente, l'autenticazione utente potrebbe comunque avere esito negativo se:

- Un utente locale con autorità **lxc-ripristino** non esiste.
- Il nome distinto radice non è corretto.
- L'utente non è membro di almeno un gruppo nel server di autenticazione esterna corrispondente al nome di un gruppo di ruoli sul server di autenticazione XClarity Administrator. XClarity Administrator non può rilevare se DN radice è corretto, ma può rilevare se un utente è membro di almeno un gruppo. Se un utente non è membro di almeno un gruppo, quando l'utente prova a eseguire il login a XClarity Administrator viene visualizzato un messaggio di errore. Per ulteriori informazioni sulla risoluzione dei problemi con i server di autenticazione esterni, vedere Problemi di connettività nella documentazione online di XClarity Administrator.

Passo 4. Creazione di un account utente esterno con accesso a XClarity Administrator:

a. Dal server di autenticazione esterna, creare un account utente. Per istruzioni, consultare la documentazione di Active Directory o OpenLDAP.

b. Creazione di un gruppo globale Active Directory o OpenLDAP con il nome di un gruppo predefinito e autorizzato. Il gruppo deve essere creato nel contesto del nome distinto radice definito nel client LDAP.

c. Aggiungere l'utente Active Directory o OpenLDAP come membro del gruppo di sicurezza creato in precedenza.

d. Accedere a XClarity Administrator utilizzando il nome utente Active Directory o OpenLDAP.

e. **Facoltativo:** definire e creare i gruppi aggiuntivi. È possibile autorizzare queste gruppi e assegnare i ruoli dalla pagina "Utenti e gruppi".

f. Se LDAP sicuro è abilitato, importare i certificati attendibili nel server LDAP esterno (vedere Installazione di un certificato del server con firma esterna personalizzato).

Risultati

XClarity Administrator convalida il collegamento del server LDAP. Se la convalida riesce, l'autenticazione utente viene effettuata sul server di autenticazione esterno quando si esegue il login a XClarity Administrator, CMM e al controller di gestione.

Se la convalida non riesce, la modalità di autenticazione viene automaticamente reimpostata su **Consenti accesso di utenti locali** e viene visualizzato un messaggio che descrive la causa dell'errore.

Nota: I gruppi di ruoli corretti devono essere configurati in XClarity Administrator e gli account utente devono essere definiti come membri di uno dei gruppi di ruoli sul server Active Directory. In caso contrario, l'autenticazione utente non riesce.

Configurazione di un provider di identità SAML esterno

È possibile scegliere di utilizzare SAML (Security Assertion Markup Language) 2.0 provider di identità per eseguire l'autenticazione e l'autorizzazione di Lenovo XClarity Administrator.

Prima di iniziare

Prima di configurare provider di identità è necessario completare la configurazione iniziale di XClarity Administrator.

Il provider di identità deve essere Microsoft Active Directory Federated Service (AD FS) e può essere connesso alla rete di gestione, alla rete di dati o a entrambe. Poiché l'autenticazione viene eseguita tramite il browser Web, il browser Web deve essere in grado di accedere a XClarity Administrator e al server SAML.

È possibile scaricare i metadati IDP utilizzando il seguente URL: `https://<ADFS_IP_Address>/federationmetadata/2007-06/federationmetadata.xml`, dove *<ADFS_IP_Address>* è l'indirizzo IP per AD FS (ad esempio, https://10.192.0.0/federationmetadata/2007-06/federationmetadata.xml).

È necessario creare o rinominare i gruppi di ruoli del server di autenticazione delle posizioni in modo che corrispondano ai gruppi definiti nel server di autenticazione esterna.

Per configurare un provider di identità SAML, è necessario essere collegati come utente membro del gruppo **lxc_admin** o **lxc_supervisor**.

Informazioni su questa attività

XClarity Administrator supporta l'utilizzo di un provider di identità Security Assertion Markup Language 2.0 per autenticare e autorizzare gli utenti. Oltre all'immissione di nome utente e password, il provider di identità può essere configurato in modo da richiedere criteri aggiuntivi per convalidare l'identità di un utente, come immissione di un codice PIN, lettura di una smart card e autenticazione mediante un certificato client.

Quando XClarity Administrator viene configurato per utilizzare un provider di identità, le richieste di login interattive dall'interfaccia Web di XClarity Administrator vengono reindirizzate al provider di identità per l'autenticazione. Una volta autenticato l'utente, il browser Web viene reindirizzato a XClarity Administrator.

Nota: se il provider di identità viene abilitato, è possibile ignorare il provider di identità ed eseguire il login a XClarity Administrator utilizzando il server di autenticazione LDAP esterna o locale, aprendo la pagina di login a XClarity Administrator dal browser Web (ad esempio, `https://<ip_address>/ui/login.htm`).

Quando XClarity Administrator è configurato per utilizzare un profilo provider di identità, la pagina "Gestione utenti" dell'interfaccia Web di XClarity Administrator non viene disabilitata. Gli account utente locali sono richiesti per eseguire direttamente il login a uno chassis gestito o al server (tranne se Incapsulamento non è abilitato su tale dispositivo) e per l'autenticazione PowerShell e API REST.

Procedura

Per configurare un provider di identità (AD FS) SAML esterno, completare le seguenti operazioni.

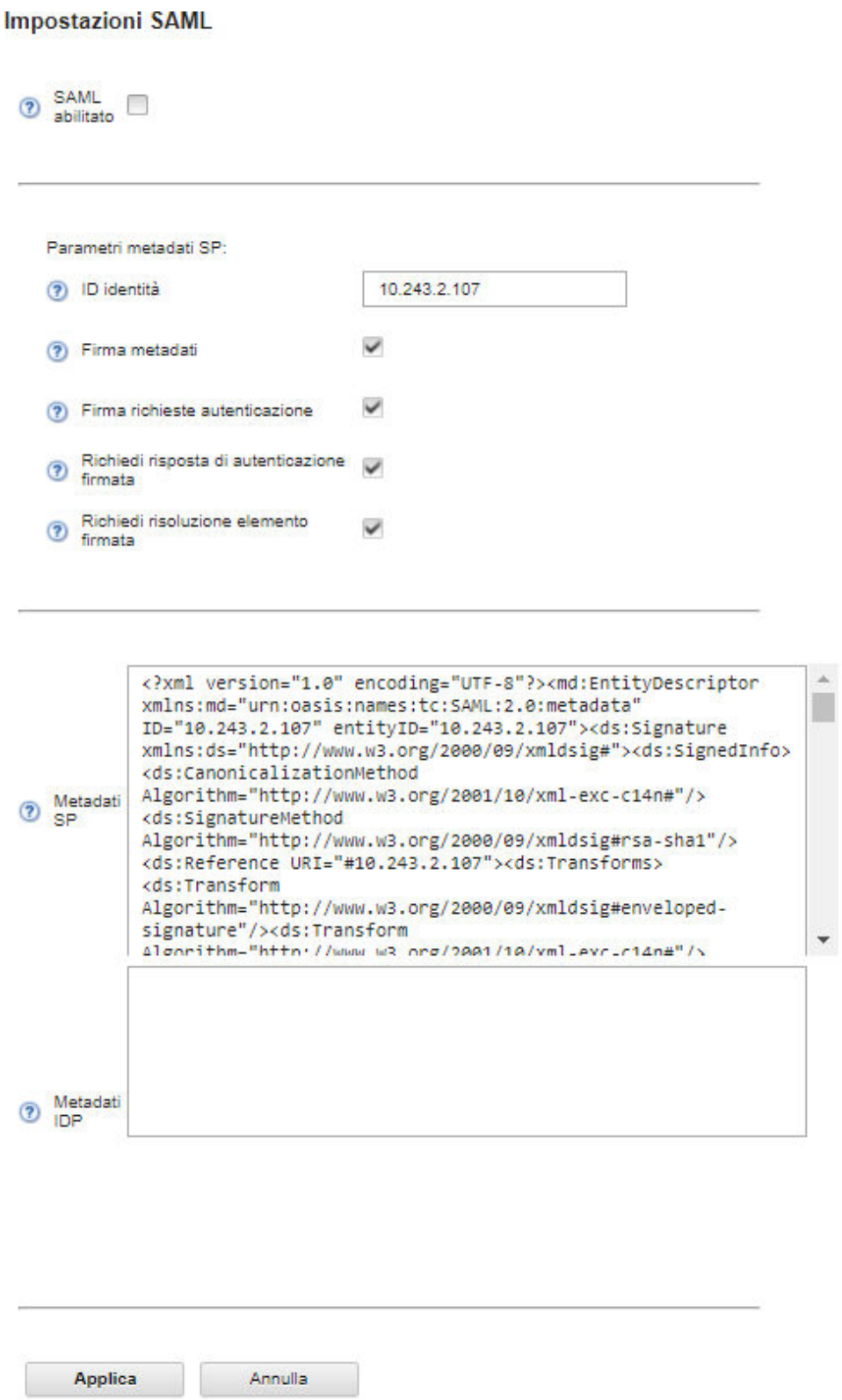
Passo 1. Creare un account utente di ripristino che può essere utilizzato per eseguire il login a XClarity Administrator se il provider di identità non è disponibile (vedere Gestione degli account utente).

Passo 2. Recuperare i metadati IDP (provider di identità) dal provider di identità e salvare il file sull'host XClarity Administrator.

Passo 3. Configurare il client SAML di XClarity Administrator.

a. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

b. Fare clic su **Impostazioni SAML** nella sezione "Utenti e gruppi" per visualizzare la finestra di dialogo Impostazioni SAML.



c. Compilare i campi nella pagina delle impostazioni SAML:

   1. Verificare che l'ID entità corrisponda all'indirizzo IP del server di gestione XClarity Administrator.
   2. Scegliere se i metadati generati devono essere firmati digitalmente.

3. Scegliere se le richieste di autenticazione devono essere firmate.
4. Scegliere se le risposte di autenticazione devono essere firmate.
5. Scegliere se le richieste di risoluzione degli elementi inviate al provider di identità remoto devono essere firmate.
6. Incollare i metadati IDP (provider di identità) SAML generati dal provider di identità e recuperati nel passaggio Passo 2 3 a pagina 26 nel campo **Metadati IDP**.

d. Fare clic su **Applica** per applicare le modifiche e aggiornare il testo nel campo Metadati SP.

Attenzione: *Non* selezionare **SAML abilitato** ora. Sarà necessario abilitare SAML in un passaggio successivo per riavviare XClarity Administrator.

e. Copiare e incollare i dati nel campo **Metadati SP** in un file e salvarlo con estensione .XML (ad esempio, sp_metadata.xml). Copiare questo file sull'host AD FS.

Passo 4. Configurare AD FS.

a. Aprire lo strumento di gestione AD FS.
b. Fare clic su **ADFS → Attendibilità relying party**.
c. Fare clic con il pulsante destro del mouse su **Attendibilità relying party**, quindi fare clic su **Aggiungi attendibilità relying party** per visualizzare la procedura guidata
d. Fare clic su **Avvia**
e. Nella pagina "Seleziona origine dati", selezionare **Importa dati sulla relying party da un file**, quindi selezionare quindi il file dei metadati SP salvato al passaggio 3e.
f. Immettere il nome visualizzato.
g. Fare clic su **Avanti** su tutte le pagine per scegliere i valori predefiniti.
h. Fare clic su **Fine** per visualizzare la pagina Regole attestazioni
i. Non modificare i valori predefiniti del campo **Invia attributi LDAP come attestazioni** e fare clic su **Avanti**.
j. Immettere un nome regole attestazioni.
k. Selezionare **Active Directory** per l'archivio di attributi.
l. Aggiungere un'associazione. Sul lato sinistro, selezionare **SAM-Account-Name** e a destra, selezionare **ID nome** per il tipo di attestazione in uscita.
m. Aggiungere un'altra associazione. Sul lato sinistro, selezionare **Token-Groups-Unqualified Names** e a destra, selezionare **Gruppo** per il tipo di attestazione in uscita
n. Fare clic su **OK**.
o. Individuare l'elemento attendibile appena creato nell'elenco di **Attendibilità relying party**.
p. Fare clic con il pulsante destro del mouse sull'elemento attendibile e scegliere **Seleziona proprietà**. Viene visualizzata la finestra "Proprietà" dell'elemento attendibile.
q. Fare clic sulla scheda **Avanzate** e selezionare `SHA-1` come algoritmo hash sicuro.

Passo 5. Salvare il certificato server da AD FS.

a. Fare clic su **Console AD FS → Assistenza → Certificati**.
b. Selezionare **Certificato** in firma di token.
c. Fare clic con il pulsante destro del mouse sul certificato e fare clic su **Visualizza certificato**.
d. Fare clic sulla scheda **Dettagli**.
e. Fare clic su **Copia su file** e salvare il certificato come file binario codificato DER X.509 (.CER).
f. Copiare il file .CER del certificato server sull'host XClarity Administrator.

Passo 6. Importare il certificato attendibile AD FS nell'interfaccia Web di XClarity Administrator.

a. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
b. Fare clic su **Certificati attendibili** nella sezione "Gestione certificati".
c. Fare clic sull'icona **Crea** ( ) per aggiungere un certificato.
d. Selezionare il file .CER del certificato server salvato al passaggio precedente.
e. Fare clic su **Crea**.

Passo 7. Fare clic su **Impostazioni SAML** nella sezione "Utenti e gruppi" per visualizzare la finestra di dialogo "Impostazioni SAML".

Passo 8. Selezionare **SAML abilitato** per abilitare la gestione degli account utente mediante un provider di identità esterno. Quando questa opzione è selezionata, tutti gli account utente esistono in remoto in un provider di identità.

Passo 9. Fare clic su **Applica** per applicare le modifiche e riavviare il server di gestione.

Passo 10. Attendere alcuni minuti per il riavvio di XClarity Administrator.

Attenzione: non riavviare l'appliance virtuale manualmente durante questo processo.

Passo 11. Chiudere e riavviare il browser Web.

Passo 12. Eseguire il login all'interfaccia Web di XClarity Administrator dal provider di identità.

Risultati

XClarity Administrator prova a verificare la configurazione per rilevare gli errori comuni. Se il test non riesce, vengono visualizzati i messaggi di errore che indicano l'origine degli errori.

XClarity Administrator convalida la connessione del provider di identità. Se la convalida viene superata, l'utente viene autenticato con il provider di identità quando si esegue il login a XClarity Administrator.

Configurazione di un sistema di gestione dell'identità esterno

Un *sistema di gestione delle identità* è un vault di password esterno che può essere utilizzato facoltativamente con Lenovo XClarity Administrator per memorizzare le credenziali di XClarity Administrator e XClarity Controller. Quando viene aggiunto un sistema di gestione delle identità a XClarity Administrator, XClarity Administrator recupera le password dal sistema di gestione delle identità, invece che dai server di autenticazione.

Informazioni su questa attività

XClarity Administrator supporta il seguente sistema di gestione delle identità.

- CyberArk

Configurazione di un sistema di gestione dell'identità CyberArk

CyberArk è un insieme di credenziali della password esterno che può essere utilizzato facoltativamente con Lenovo XClarity Administrator per memorizzare le credenziali di XClarity Administrator e Lenovo XClarity Controller. Una volta memorizzata una password di un account in CyberArk, la password viene gestita da CyberArk

Informazioni su questa attività

XClarity Administrator consente di memorizzare le password XCC in sistemi di gestione delle identità forniti da CyberArk, un servizio di terze parti. Lenovo non è responsabile del servizio CyberArk e l'utente è responsabile del rapporto diretto con CyberArk.

Se gli account utente per un server ThinkSystem o ThinkAgile sono integrati in CyberArk, è possibile scegliere di utilizzare XClarity Administrator per recuperare le credenziali tramite CyberArk al fine di accedere

al server durante la configurazione iniziale dei server per la gestione (con autenticazione gestita o locale). Prima che le credenziali possano essere recuperate da CyberArk, i percorsi CyberArk devono essere definiti in XClarity Administrator e l'attendibilità reciproca deve essere stabilita tra CyberArk e XClarity Administrator utilizzando l'autenticazione TLS reciproca tramite i certificati client.

Procedura

Per configurare XClarity Administrator per utilizzare CyberArk, completare la seguente procedura.

Passo 1. Configurare CyberArk.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
2. Fare clic su **CyberArk** nella sezione Gestione identità.
3. Fare clic su **Modifica dettagli server CyberArk** dalla barra degli strumenti.
4. Specificare il nome host o l'indirizzo IP e il numero di porta CyberArk.
5. Fare clic su **Applica**.

Passo 2. Importare il certificato di autenticazione reciproca di XClarity Administrator in CyberArk.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
2. Fare clic su **Certificato server** nella sezione Gestione certificati.
3. Fare clic sulla scheda **Certificato client**.
4. Selezionare **CyberArk** come tipo di server.
5. Fare clic su **Rigenera certificato** per generare un nuovo certificato di autenticazione reciproca TLS per CyberArk.

   Attenzione: Se si rigenera il certificato di autenticazione reciproca TLS per CyberArk dopo aver stabilito una connessione tra XClarity Administrator e CyberArk, la connessione andrà persa finché non verrà importato il nuovo certificato in CyberArk.
6. Fare clic su **Scarica certificato** e quindi su **Salva come DER** o **Salva come PEM** per salvare il file del certificato nel sistema locale.
7. Importare il certificato scaricato in CyberArk.

Passo 3. Importare il certificato CA radice di CyberArk in XClarity Administrator.

1. Scaricare il certificato CA radice da CyberArk.
2. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
3. Fare clic su **Certificati attendibili** nella sezione "Gestione certificati".
4. Fare clic sull'icona **Crea** ( ) per aggiungere un certificato.
5. Individuare il file o incollare il testo del certificato con formattazione PEM.
6. Fare clic su **Crea**.

Passo 4. Aggiungere i percorsi che identificano la posizione degli account utente integrati in CyberArk.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
2. Fare clic su **CyberArk** nella sezione Gestione identità.
3. Fare clic sulla scheda **Percorsi**.
4. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo Crea percorso CyberArk.

5. Facoltativamente specificare l'ID applicazione, la cassaforte e la cartella in cui gli account utente vengono memorizzati in CyberArk.

   Se viene specificato l'ID dell'applicazione e la cassaforte e, facoltativamente, la cartella, XClarity Administrator tenta di trovare l'account utente nella posizione indicata.

   Se viene specificata una combinazione di campi diversi da ID applicazione e cassaforte (ad esempio, solo l'ID applicazione, solo la cassaforte e la cartella o solo l'ID applicazione e la cartella), in XClarity Administrator il percorso viene filtrato utilizzando i valori indicati.
6. Fare clic su **Applica**.

Al termine

- Modificare un percorso CyberArk selezionato facendo clic sull'icona **Modifica** ( ).
- Eliminare un percorso CyberArk selezionato facendo clic sull'icona **Elimina** ( ).

Determinazione del tipo di metodo di autenticazione utilizzato da Lenovo XClarity Administrator

È possibile determinare il tipo di metodo di autenticazione attualmente utilizzato tramite le schede **Client LDAP** e **Impostazioni SAML** della pagina "Sicurezza".

Informazioni su questa attività

Il *server di autenticazione* è un registro utente utilizzato per autenticare le credenziali utente. Lenovo XClarity Administrator supporta i seguenti tipi di server di autenticazione.

- **Server di autenticazione locale**. Per impostazione predefinita, XClarity Administrator è configurato per utilizzare il server LDAP (Lightweight Directory Access Protocol) che risiede nel server di gestione.
- **Server LDAP esterno**. Attualmente, solo Microsoft Active Directory e OpenLDAP sono supportati. Questo server deve trovarsi in un server Microsoft Windows esterno connesso alla rete di gestione. Quando viene utilizzato un server LDAP esterno, il server di autenticazione locale è disabilitato.

  Attenzione: Per configurare il metodo di collegamento Active Directory in modo da utilizzare le credenziali di login, il firmware del controller BMC (Baseboard Management Controller) di ciascun server gestito deve essere aggiornato a settembre 2016 o successivo.
- **Sistema di gestione delle identità esterno**. Attualmente è supportato solo CyberArk.

  Se gli account utente per un server ThinkSystem o ThinkAgile sono integrati in CyberArk, è possibile scegliere di utilizzare XClarity Administrator per recuperare le credenziali tramite CyberArk al fine di accedere al server durante la configurazione iniziale dei server per la gestione (con autenticazione gestita o locale). Prima che le credenziali possano essere recuperate da CyberArk, i percorsi CyberArk devono

essere definiti in XClarity Administrator e l'attendibilità reciproca deve essere stabilita tra CyberArk e XClarity Administrator utilizzando l'autenticazione TLS reciproca tramite i certificati client.

- **SAML esterno provider di identità**. Attualmente, è supportato solo Microsoft Active Directory Federation Services (AD FS). Oltre all'immissione di un nome utente e una password, l'autenticazione a più fattori può essere configurata in modo da garantire un'ulteriore protezione attraverso la richiesta di un codice PIN, la lettura di una smart card e un certificato client. Quando viene utilizzato un provider di identità SAML, il server di autenticazione locale non viene disabilitato. Gli account utente locali sono richiesti per accedere direttamente a uno chassis gestito o al server (tranne se Incapsulamento non è abilitato su tale dispositivo), per l'autenticazione PowerShell e API REST, nonché per il ripristino se l'autenticazione esterna non è disponibile.

  È possibile scegliere di utilizzare sia un server LDAP esterno che un provider di identità esterno. Se entrambi sono abilitati, il server LDAP esterna viene utilizzato per accedere direttamente ai dispositivi da gestire, mentre il provider di identità viene utilizzato per accedere al server di gestione.

Procedura

Per determinare il tipo di server di autenticazione utilizzato dal software di gestione, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 2. Fare clic su **Client LDAP** nella sezione "Utenti e gruppi" per visualizzare la finestra di dialogo Impostazioni client LDAP.

Verificare il metodo di autenticazione utente selezionato:

- **Consenti accesso di utenti locali**. L'autenticazione viene eseguita utilizzando l'autenticazione locale. Se questa opzione è selezionata, tutti gli account utente sono disponibili nel server di autenticazione locale sul nodo di gestione.
- **Consenti accesso di utenti LDAP**. L'autenticazione viene eseguita da un server LDAP esterno. Questo metodo consente la gestione remota degli account utente. Quando questa opzione è selezionata, tutti gli account utente esistono in remoto su un server LDAP esterno.
- **Consenti prima l'accesso degli utenti locali, quindi degli utenti LDAP**. Il server di autenticazione locale esegue prima l'autenticazione. In caso di errore, l'autenticazione viene eseguita da un server LDAP esterno.
- **Consenti prima utenti LDAP, poi utenti locali**. Un server LDAP esterno esegue prima l'autenticazione. In caso di errore, l'autenticazione viene eseguita dal server di autenticazione locale.

Passo 3. Fare clic su **Impostazioni SAML** nella sezione "Utenti e gruppi" per visualizzare la pagina "Impostazioni SAML".

Se l'opzione **SAML abilitato** è selezionata, provider di identità viene utilizzato.

Accesso a Lenovo XClarity Administrator in seguito a un errore del server LDAP esterno

Se si utilizza un server di autenticazione LDAP esterno e tale server non è disponibile, attenersi alla procedura riportata di seguito per ripristinare l'accesso all'interfaccia Web di Lenovo XClarity Administrator utilizzando il server di autenticazione locale sul nodo di gestione.

Procedura

Per modificare le impostazioni del client LDAP, effettuare le operazioni riportate di seguito.

Passo 1. Eseguire il login all'interfaccia Web di XClarity Administrator mediante un account utente con autorità **lxc-ripristino**. Per ulteriori informazioni sul nome di dominio del client, vedere Configurazione di un server di autenticazione LDAP esterno.

Passo 2. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 3. Fare clic su **Client LDAP** nella sezione "Utenti e gruppi" per visualizzare la finestra di dialogo Client LDAP.

Passo 4. Selezionare **Consenti accesso di utenti locali** per il metodo di autenticazione utente in modo da abilitare la gestione locale degli account utente. Se questa opzione è selezionata, tutti gli account utente sono disponibili in locale sul server di gestione.

Passo 5. Fare clic su **Applica**.

Risultati

Ora è possibile utilizzare gli account utente nel server di autenticazione locale per accedere al server di gestione di XClarity Administrator. Una volta che il server di autenticazione esterna è stato ripristinato e reso disponibile per il server di gestione, è possibile reimpostare la configurazione del client LDAP su "Server di autenticazione esterna".

Accesso a Lenovo XClarity Administrator in seguito a un errore provider di identità SAML esterno

Se si utilizza un provider di identità SAML esterno e tale server è guasto o non è disponibile, attenersi alla procedura riportata di seguito per ripristinare l'accesso all'interfaccia Web di Lenovo XClarity Administrator utilizzando il server di autenticazione locale XClarity Administrator.

Procedura

Per modificare le impostazioni del client SAML, effettuare le seguenti operazioni.

Passo 1. Aprire la pagina di login di XClarity Administrator nel browser Web (ad esempio, `https://<ip_address>/ui/login.html`).

Passo 2. Eseguire il login all'interfaccia Web di XClarity Administrator utilizzando un account utente di ripristino locale, creato durante la configurazione del provider di identità.

Passo 3. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 4. Fare clic su **Impostazioni SAML** nella sezione "Utenti e gruppi" per visualizzare la finestra di dialogo Impostazioni SAML.

Passo 5. Deselezionare **Abilita SAML** per disabilitare il provider di identità SAML. Se questa opzione non è selezionata, il server di autenticazione locale o il server LDAP esterno (se configurato) viene utilizzato per l'autenticazione.

Passo 6. Fare clic su **Applica**.

Risultati

Ora è possibile utilizzare gli account utente nel server di autenticazione locale per accedere al server di gestione di XClarity Administrator. Una volta ripristinato e reso disponibile il provider di identità esterno al server di gestione, è possibile modificare il metodo di autenticazione in provider di identità.

Gestione degli account utente

Gli *account utente* sono utilizzati per eseguire il login e gestire Lenovo XClarity Administrator, nonché tutti gli chassis e i server gestiti da XClarity Administrator. Gli account utente di XClarity Administrator sono soggetti a due processi interdipendenti: autenticazione e autorizzazione.

Informazioni su questa attività

L'*autenticazione* è il meccanismo di sicurezza che consente di verificare le credenziali degli utenti. Il processo di autenticazione utilizza le credenziali utente memorizzate nel server di autenticazione configurato. Esso impedisce alle applicazioni dei sistemi gestiti o ai server di gestione non autorizzati di accedere alle risorse. Una volta autenticato, un utente può accedere a XClarity Administrator. Tuttavia, per accedere a una risorsa specifica o per eseguire una determinata attività, l'utente deve anche disporre dell'autorizzazione appropriata.

L'*autorizzazione* verifica le autorizzazioni dell'utente autenticato e controlla l'accesso alle risorse in base all'appartenenza degli utenti a un gruppo di ruoli. I *gruppi di ruoli* vengono utilizzati per assegnare ruoli specifici a una serie di account utente definiti e gestiti nel server di autenticazione. Ad esempio, se un utente è membro di un gruppo di ruoli con autorizzazioni di supervisore può creare, modificare ed eliminare gli account utente da XClarity Administrator. Se un utente dispone delle autorizzazioni di operatore può solo visualizzare le informazioni sull'account utente.

Nota: Gli account utente SYSMGR_* e SYSRDR_* (dove * è un suffisso che viene scelto casualmente tra i caratteri A - Z e 0 - 9) vengono generati e utilizzati da XClarity Administrator come account utente del servizio e utilizzati in funzioni, quali autenticazione gestita, distribuzione del sistema operativo e aggiornamenti firmware. Le password SYSMGR_* e SYSRDR_* vengono ruotate ogni volta che viene avviato XClarity Administrator e subito prima della scadenza del periodo di validità delle password.

Creazione di un utente

Gli account utente sono utilizzati per gestire l'autorizzazione e l'accesso alle risorse.

Informazioni su questa attività

Il primo account utente creato deve disporre del ruolo da supervisore e deve essere attivato (abilitato).

Come misura aggiuntiva di sicurezza, creare almeno due account utente con il ruolo **Supervisore**. Assicurarsi di registrare le password per questi account utente e memorizzarle in un'ubicazione sicura nel caso sia necessario ripristinare Lenovo XClarity Administrator.

Procedura

Per aggiungere un utente a XClarity Administrator, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 2. Fare clic su **Utenti locali** nella sezione Utenti e gruppi per visualizzare la pagina Gestione utenti.

Passo 3. Fare clic sull'icona **Crea** ( ) per creare un utente. Viene visualizzata la finestra di dialogo Crea nuovo utente.

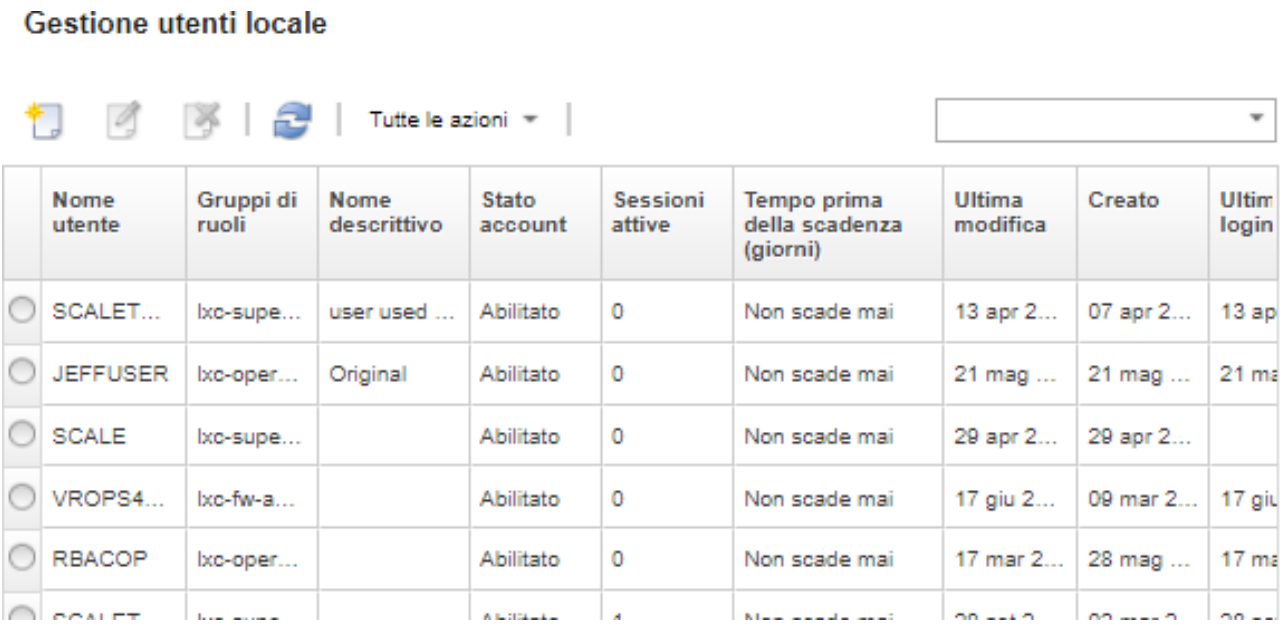
Passo 4. Compilare le seguenti informazioni nella finestra di dialogo.

- Immettere un nome utente e una descrizione per l'utente stesso.
- Immettere e confermare le nuove password. Le regole per le password sono basate sulle impostazioni correnti di sicurezza dell'account.
- Selezionare uno o più gruppi di ruoli per autorizzare l'utente ad eseguire le attività appropriate. Per informazioni sui gruppi di ruoli e su come creare gruppi di ruoli personalizzati, vedere Creazione di un gruppo di ruoli personalizzato.
- (Facoltativo) Impostare **Modifica password al primo accesso** su `Yes` se si desidera forzare l'utente a modificare la password quando esegue per la prima volta il login a XClarity Administrator.

Passo 5. Fare clic su **Crea**.

Al termine

L'account utente viene visualizzato nella tabella Gestione utenti. La tabella mostra i gruppi di ruoli associati e lo stato dell'account per ogni account utente.



Dopo aver creato un account utente, è possibile eseguire le seguenti azioni su un account utente selezionato:

- Modificare il nome utente, la descrizione e il ruolo per un account utente facendo clic sull'icona **Modifica** ( ).
- Eliminare l'account utente facendo clic sull'icona **Elimina** ( ).
- Reimpostare la password per l'account utente (vedere Reimpostazione della password per un utente).
- Sbloccare l'account (vedere Sblocco di un utente).
- Abilitare o disabilitare un account utente (vedere Abilitazione o disabilitazione di un utente).

Abilitazione o disabilitazione di un utente

È possibile modificare l'abilitazione o la disabilitazione di un account utente locale nel server di autenticazione.

Procedura

Per abilitare o disabilitare un account utente, completare le seguenti operazioni.

- Se si utilizza il server di autenticazione locale:
  1. Dalla barra del titolo di Lenovo XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
  2. Fare clic su **Utenti locali** nella sezione Utenti e gruppi per visualizzare la pagina Gestione utenti.
  3. Selezionare un account utente.
  4. Se l'account utente è abilitato, fare clic su **Tutte le azioni → Disabilita account selezionato** per disabilitare l'utente. Lo stato dell'account nella tabella viene modificato in `Disabled`.
  5. Se l'account utente è disabilitato, fare clic su **Tutte le azioni → Abilita account selezionato** per abilitare l'utente. Lo stato dell'account nella tabella viene modificato in `Enabled`.
- Se si utilizza un server LDAP esterno, abilitare o disabilitare un account utente in Microsoft Active Directory.

- Se si utilizza un provider di identità SAML esterno, abilitare o disabilitare un account utente nel provider di identità.

Disconnessione di un utente attivo

È possibile disconnettere (terminare) un utente attivo da Lenovo XClarity Administrator.

È necessario essere collegati a XClarity Administrator mediante un account utente con autorità **lxc-supervisor** o **lxc-security-admin**.

Procedura

Per disconnettere un utente attivo, completare le seguenti operazioni.

Passo 1. Dalla barra del titolo di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 2. Fare clic su **Sessioni attive** nella sezione Utenti e gruppi per visualizzare la pagina Gestione sessioni attive.

Passo 3. Selezionare uno o più account utente.

Passo 4. Fare clic su **Disconnetti utente**.

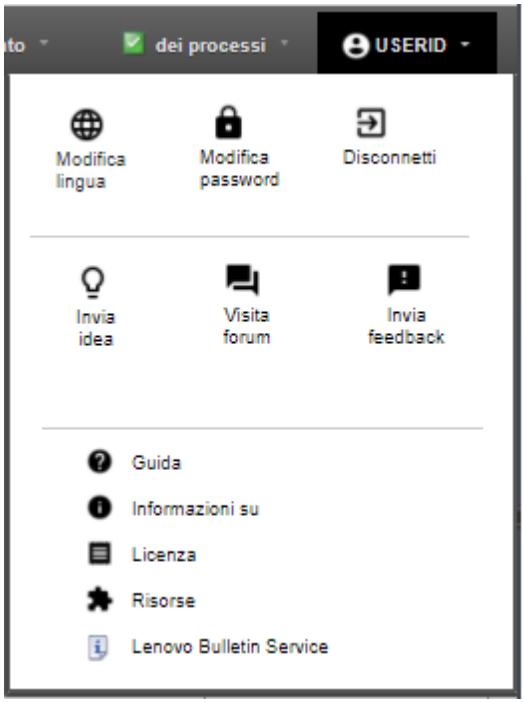
Modifica della password per l'account utente

È possibile modificare la password per l'account utente.

Procedura

Completare le seguenti operazioni per modificare la password.

- Se si utilizza il server di autenticazione locale:
  1. Nella barra del titolo di Lenovo XClarity Administrator, fare clic sul menu azioni utente (ADMIN_USER) e quindi su **Modifica password**. Viene visualizzata la finestra di dialogo Modifica password.



  2. Immettere la password corrente.

3. Immettere e confermare le nuove password. Le regole per le password sono basate sulle impostazioni correnti di sicurezza dell'account.
4. Fare clic su **Modifica**.

- Se si utilizza un server di autenticazione esterna, modificare la password in Microsoft Active Directory.

  Attenzione: Se si aggiorna Microsoft Active Directory con una nuova password per l'account client utilizzato per collegare XClarity Administrator al server di autenticazione esterna, accertarsi di aggiornare la password anche nell'interfaccia Web di XClarity Administrator (vedere Configurazione di un server di autenticazione LDAP esterno).
- Se si utilizza un provider di identità SAML esterno, modificare la password nel provider di identità.

Reimpostazione della password per un utente

È possibile reimpostare la password per qualsiasi account utente.

Procedura

Per reimpostare una password, completare le seguenti operazioni.

- Se si utilizza il server di autenticazione locale, reimpostare la password dall'interfaccia Web di Lenovo XClarity Administrator:
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
  2. Fare clic su **Utenti locali** nella sezione Utenti e gruppi per visualizzare la pagina Gestione utenti.
  3. Selezionare un account utente dalla tabella.
  4. Se l'account utente è abilitato, fare clic su **Tutte le azioni → Reimposta password per l'utente selezionato**. Viene visualizzata la finestra di dialogo Reimposta password.
     a. Immettere e confermare le nuove password. Le regole per le password sono basate sulle impostazioni correnti di sicurezza dell'account.
     b. Facoltativamente, impostare **Modifica al primo accesso** su `Yes` se si desidera forzare l'utente a modificare la password quando esegue per la prima volta il login a XClarity Administrator.
     c. Fare clic su **Reimposta**.
- Se si utilizza un server LDAP esterno, reimpostare la password in Microsoft Active Directory.
- Se si utilizza un provider di identità SAML esterno, reimpostare la password nel provider di identità.
- Se non è possibile eseguire il login a XClarity Administrator mediante un altro account supervisore o se un altro account supervisore non esiste, è possibile reimpostare la password per un utente locale con autorità di ripristino o supervisore montando un'immagine ISO che contiene un file di configurazione con la nuova password. Per ulteriori informazioni, vedere Password per il ripristino locale o un utente supervisore dimenticata nella documentazione online di XClarity Administrator.

Sblocco di un utente

È possibile sbloccare un account utente bloccato da Lenovo XClarity Administrator. Un account utente può risultare temporaneamente bloccato se l'utente tenta troppi login non validi.

Informazioni su questa attività

Le impostazioni di sicurezza dell'account utente controllano l'intervallo minimo di tempo (espresso in minuti) che deve trascorrere prima che un utente precedentemente bloccato possa provare nuovamente ad eseguire il login. Se **Periodo di blocco in seguito al numero massimo di errori di login** è impostato su `0`, l'account utente rimane bloccato finché non viene sbloccato in modo esplicito dall'amministratore. Per ulteriori informazioni sul periodo di blocco per il numero massimo di errori di login, vedere Modifica delle impostazioni di sicurezza dell'account utente.

È inoltre possibile disabilitare o abilitare in modo permanente un account utente. Per ulteriori informazioni, vedere Abilitazione o disabilitazione di un utente.

Nota: È necessario disporre dei privilegi di supervisore per sbloccare un account utente.

Suggerimento: è possibile utilizzare XClarity Administrator per sbloccare gli account utente gestiti mediante il server di autenticazione locale. Non è possibile sbloccare gli account utente in un server di autenticazione esterna mediante XClarity Administrator.

Procedura

Per sbloccare un account utente, completare le seguenti operazioni.

- Se si utilizza il server di autenticazione locale:
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
  2. Fare clic su **Utenti locali** nella sezione Utenti e gruppi per visualizzare la pagina Gestione utenti.
  3. Selezionare l'account utente dalla tabella.
  4. Selezionare **Tutte le azioni → Sblocca account per l'utente selezionato**.
- Se si utilizza un server LDAP esterno, sbloccare l'account utente in Microsoft Active Directory.
- Se si utilizza un provider di identità SAML esterno, sbloccare l'account utente nel provider di identità.

Monitoraggio degli utenti attivi

È possibile determinare chi è collegato all'interfaccia Web di Lenovo XClarity Administrator dalla pagina Dashboard.

Procedura

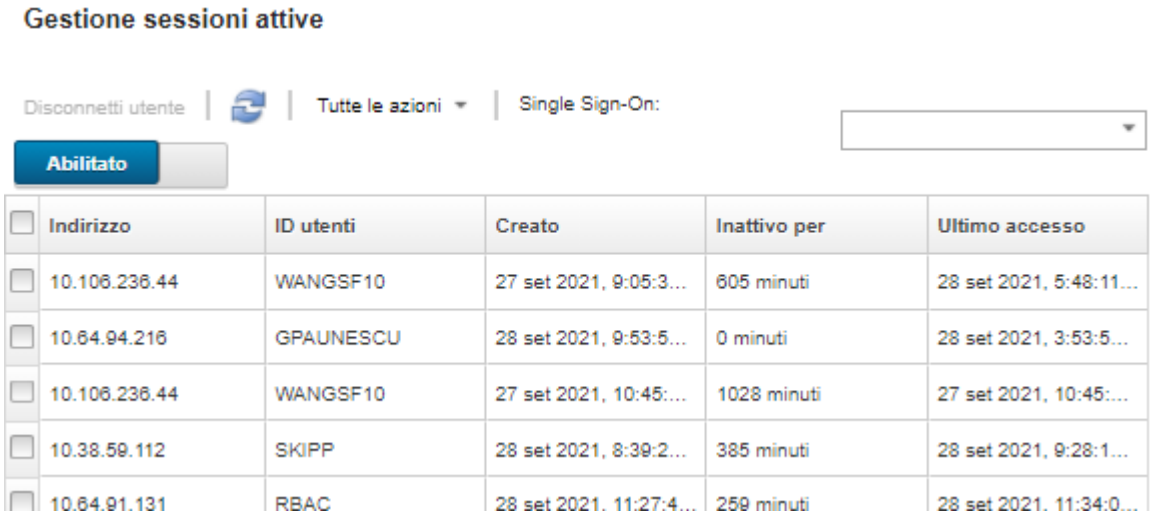
- È possibile ottenere un elenco degli utenti attivo e i relativi indirizzi IP facendo clic su **Dashboard** dalla barra di menu di XClarity Administrator.

  Le sessioni utente attive sono elencate nella sezione "Attività".

- È possibile ottenere un elenco di tutti gli utenti attivi (diversi dall'utente corrente) e i relativi indirizzi IP facendo clic su **Amministrazione → Sicurezza** dalla barra dei menu di XClarity Administrator e facendo quindi clic su **Sessioni attive**.

  Nota: Le sessioni utente inattive che superano il periodo di tempo specificato vengono disconnesse automaticamente. Per impostare il periodo di inattività fare clic su **Amministrazione → Sicurezza** dalla barra dei menu di XClarity Administrator. Quindi fare clic su "Impostazioni di sicurezza dell'account" e

modificare il valore **Timeout sessione di inattività Web**. Tenere presente che la modifica non ha effetto sulle sessioni attive. Riguarda solo le sessioni utente avviate dopo avere modificato l'impostazione.



Gestione delle credenziali memorizzate

Le *credenziali memorizzate* vengono utilizzate per gestire l'autorizzazione e l'accesso allo chassis e ai server gestiti da Lenovo XClarity Administrator mediante l'autenticazione locale.

Prima di iniziare

È necessario disporre dell'autorità **lxc-supervisor** o **lxc-security-admin** per creare, modificare o eliminare le credenziali memorizzate.

Informazioni su questa attività

Una credenziale memorizzata deve essere un account utente locale su un dispositivo o un account utente in un server Active Directory.

Se si sceglie di gestire i dispositivi utilizzando l'autenticazione locale invece dell'autenticazione gestita di XClarity Administrator, è necessario selezionare un account con credenziali memorizzate durante il processo di gestione.

Importante: XClarity Administrator non convalida il nome utente e la password specificate per la credenziale memorizzata. È responsabilità dell'utente verificare che le informazioni specificate corrispondano a un account utente attivo sul dispositivo locale o in Active Directory (se il dispositivo gestito è configurato per l'utilizzo di Active Directory per l'autenticazione).

Attenzione: Le credenziali memorizzate devono disporre dell'accesso supervisore o dell'autorità sufficiente per eseguire modifiche della configurazione sul dispositivo. Se si tenta di gestire un server con credenziali memorizzate che non dispongono di livelli sufficienti di autorizzazione sul dispositivo, il processo di gestione potrebbe avere esito positivo ma le azioni aggiuntive dell'inventario amministrativo sul dispositivo potrebbero non riuscire a causa di errori di accesso negato, che potrebbero determinare problemi di connettività con il dispositivo.

Procedura

Per aggiungere una credenziale memorizzata a XClarity Administrator, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**. Verrà visualizzata la pagina Sicurezza.

Passo 2. Fare clic su **Credenziali memorizzate** nella sezione "Autenticazione gestita" per visualizzare la pagina "Credenziale memorizzata".

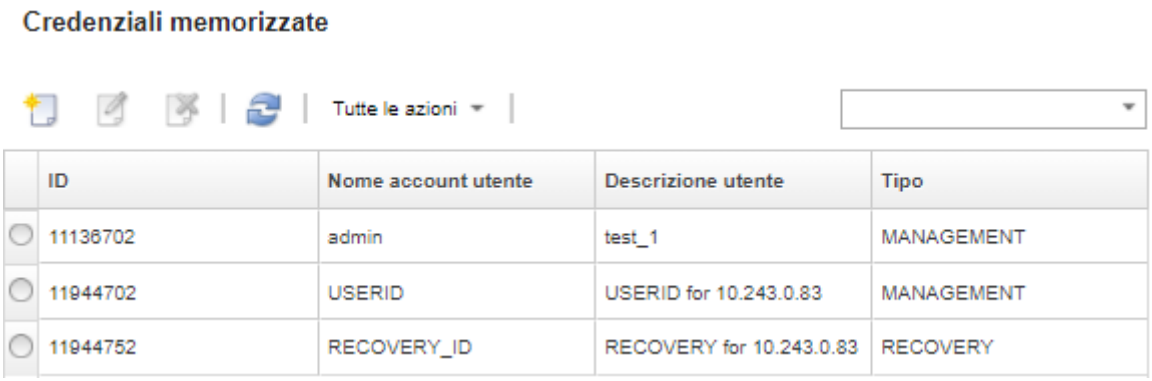
Passo 3. Fare clic sull'icona **Crea** ( ) per creare una credenziale memorizzata. Viene visualizzata la finestra di dialogo Crea nuove credenziali memorizzate.

Passo 4. Compilare le seguenti informazioni nella finestra di dialogo.
- Immettere un nome utente e una descrizione facoltativa per la credenziale memorizzata.
- Immettere e quindi confermare la password per la credenziale memorizzata.
- Facoltativamente, immettere e confermare la password per le credenziali di ripristino RECOVERY_ID memorizzate.

Passo 5. Fare clic su **Crea credenziale memorizzata**.

Al termine

L'account con la credenziale memorizzata viene visualizzato nella tabella "Credenziale memorizzata". La tabella mostra l'ID associato e una descrizione per ogni account con credenziale memorizzata.



Dalla pagina "Credenziali memorizzate", è possibile eseguire le seguenti azioni su un account con credenziali memorizzate selezionato:

- Modificare il nome utente, la password e la descrizione per un account con credenziali memorizzate, facendo clic sull'icona **Modifica** ( ).

  Nota: Se si gestisce un dispositivo utilizzando una credenziale memorizzata e si abilita l'autenticazione gestita, non è possibile modificare la credenziale memorizzata.

- Eliminare l'account con credenziali memorizzate facendo clic sull'icona **Elimina** ( ).

Per risolvere le credenziali memorizzate scadute o non valide, vedere Risoluzione di credenziali memorizzate scadute o non valide per un server.

Gestione di ruoli e gruppi di ruoli

Un *ruolo* viene utilizzato per controllare l'accesso utente alle risorse e limitare le azioni che gli utenti possono eseguire sulle risorse. Un *gruppo di ruoli* è una raccolta di uno o più ruoli che viene utilizzata per assegnare i ruoli a più utenti. I ruoli configurati per un gruppo di ruoli determinano il livello di accesso concesso a ciascun utente membro di questo gruppo di ruoli. Ogni utente Lenovo XClarity Administrator deve essere membro di almeno un gruppo di ruoli.

Creazione di un ruolo personalizzato

Un *ruolo* è un insieme di *privilegi* o di autorizzazioni per eseguire un'azione specifica. Lenovo XClarity Administrator include diversi ruoli predefiniti. È inoltre possibile creare ruoli personalizzati che applicano un insieme univoco di privilegi che gli utenti possono eseguire

Prima di iniziare

È necessario disporre dell'autorità **lxc-supervisor** o **lxc-security-admin** per eseguire questa attività.

Informazioni su questa attività

Per creare un ruolo personalizzato, selezionare uno o più ruoli predefiniti il cui ambito è più simile al ruolo che si desidera creare, quindi cancellare i singoli privilegi da limitare. In questo modo è possibile ottenere tutti i privilegi previsti e avere la certezza che il ruolo sia creato correttamente con privilegi dipendenti.

Alcuni privilegi di XClarity Administrator dipendono dai corrispondenti privilegi del modulo di gestione per eseguire azioni sui dispositivi gestiti (vedere Privilegi del modulo di gestione v1 e Privilegi del modulo di gestione v2). Un privilegio di XClarity Administrator potrebbe consentire di richiedere un'azione su un dispositivo gestito, ma il dispositivo negherà la richiesta se non si dispone dei corrispondenti privilegi per CMM, IMM o XCC. Ad esempio, se si crea un ruolo personalizzato per eseguire azioni di accensione e spegnimento sui dispositivi gestiti, è possibile aggiungere il privilegio **lxc-inventory-modify-device-power-state** e:

- Per un server ThinkSystem in un rack, aggiungere il privilegio **mm-power-and-restart-access-v1**.
- Per un intero chassis Flex System (inclusi i dispositivi nello chassis), aggiungere il privilegio **mm-power-and-restart-access-v1**.
- Per un server ThinkSystem in uno chassis, aggiungere i privilegi **mm-power-and-restart-access-v1**, **mm-blade-operator-v2** e **mm-blade-#-scope-v2** corrispondenti al server di destinazione.

Tutti i ruoli contengono privilegi di sola lettura. Nessun ruolo personalizzato è più restrittivo del ruolo **lxc-operator**.

Se un utente non dispone dei privilegi per eseguire azioni specifiche, le voci di menu, le icone della barra degli strumenti e i pulsanti che consentono di eseguire tali azioni saranno disabilitati (evidenziati in grigio).

XClarity Administrator fornisce un gruppo di ruoli per ogni ruolo predefinito, utilizzando lo stesso nome del ruolo. Valutare la possibilità di creare un gruppo di ruoli per i nuovi ruoli creati. Per ulteriori informazioni sui gruppi di ruoli, vedere Creazione di un gruppo di ruoli personalizzato.

- **lxc-supervisor**. Gli utenti assegnati a questo ruolo possono accedere, configurare ed eseguire tutte le operazioni disponibili sul server di gestione e su tutti i dispositivi gestiti.Gli utenti assegnati a questo ruolo possono sempre accedere a tutti i dispositivi gestiti. Non è possibile limitare l'accesso ai dispositivi per questo ruolo.
- **lxc-admin**. Gli utenti assegnati a questo ruolo possono modificare le impostazioni ed eseguire le operazioni non correlate alla sicurezza sul server di gestione, come la possibilità di aggiornare e riavviare il server di gestione. Questo ruolo inoltre offre la possibilità di visualizzare tutte le informazioni su configurazione e stato del server di gestione e dei dispositivi gestiti.
- **lxc-security-admin**. Gli utenti assegnati a questo ruolo possono modificare le impostazioni di sicurezza ed eseguire le operazioni correlate sul server di gestione e sui dispositivi gestiti. Questo ruolo inoltre offre la possibilità di visualizzare tutte le informazioni su configurazione e stato del server di gestione e dei dispositivi gestiti.

  Gli utenti assegnati a questo ruolo possono sempre accedere a tutti i dispositivi gestiti. Non è possibile limitare l'accesso ai dispositivi per questo ruolo.
- **lxc-hw-admin**. Gli utenti assegnati a questo ruolo possono modificare le impostazioni ed eseguire le operazioni non correlate alla sicurezza sui dispositivi gestiti, come la possibilità di aggiornare e riavviare i

dispositivi gestiti. Questo ruolo inoltre offre la possibilità di visualizzare tutte le informazioni su configurazione e stato del server di gestione e di tutti i dispositivi gestiti.
- **lxc-fw-admin**. Gli utenti assegnati a questo ruolo possono creare criteri firmware e distribuirli ai dispositivi gestiti. Gli utenti non assegnati a questo ruolo possono solo visualizzare le informazioni sui criteri.
- **lxc-os-admin**. Gli utenti assegnati a questo ruolo possono scaricare e distribuire i sistemi operativi e gli aggiornamenti dei driver di dispositivo sui server gestiti. Gli utenti non assegnati a questo ruolo possono visualizzare solo le informazioni relative al sistema operativo e ai driver di dispositivo.
- **lxc-service-admin**. Gli utenti assegnati a questo ruolo possono raccogliere e scaricare i file di servizio per XClarity Administrator e i dispositivi gestiti. Gli utenti non assegnati a questo ruolo possono raccogliere ma non scaricare i dati di servizio.
- **lxc-hw-manager**. Gli utenti assegnati a questo ruolo possono rilevare nuovi dispositivi e collocarli sotto il controllo gestionale di XClarity Administrator. Questo ruolo impedisce agli utenti di eseguire operazioni o di modificare le impostazioni delle configurazioni sul server di gestione e sui dispositivi gestiti che non rientrano nelle operazioni necessarie per rilevare e gestire nuovi dispositivi.
- **lxc-operator**. Gli utenti assegnati a questo ruolo possono visualizzare tutte le informazioni su configurazione e stato relative al server di gestione e ai dispositivi gestiti. Questo ruolo impedisce agli utenti di eseguire operazioni o di modificare le impostazioni delle configurazioni sul server di gestione e sui dispositivi gestiti.
- **lxc-recovery**. Gli utenti assegnati a questo ruolo possono modificare le impostazioni di sicurezza ed eseguire le operazioni correlate sul server di gestione. Questi utenti possono inoltre eseguire l'autenticazione diretta a XClarity Administrator, anche se il metodo di autenticazione è impostato su server LDAP esterno. Questo ruolo fornisce un meccanismo di ripristino in caso di errore di comunicazione con il server LDAP esterno che utilizza la configurazione "Credenziali di login".

  Gli utenti assegnati a questo ruolo possono sempre accedere a tutti i dispositivi gestiti. Non è possibile limitare l'accesso ai dispositivi per questo ruolo.

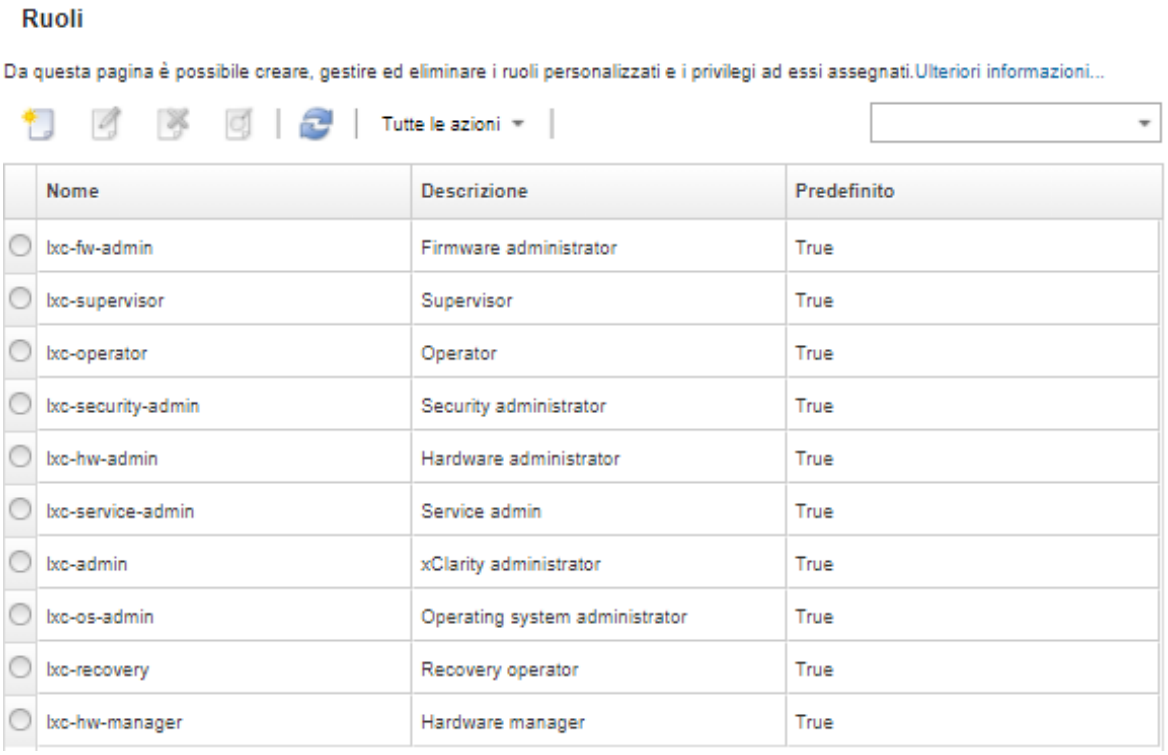
I seguenti ruoli predefiniti sono *riservati* e non possono essere utilizzati per creare nuovi gruppi di ruoli o assegnati a nuovi utenti.
- **lxc-sysrdr**
- **lxc-sysmgr**

Procedura

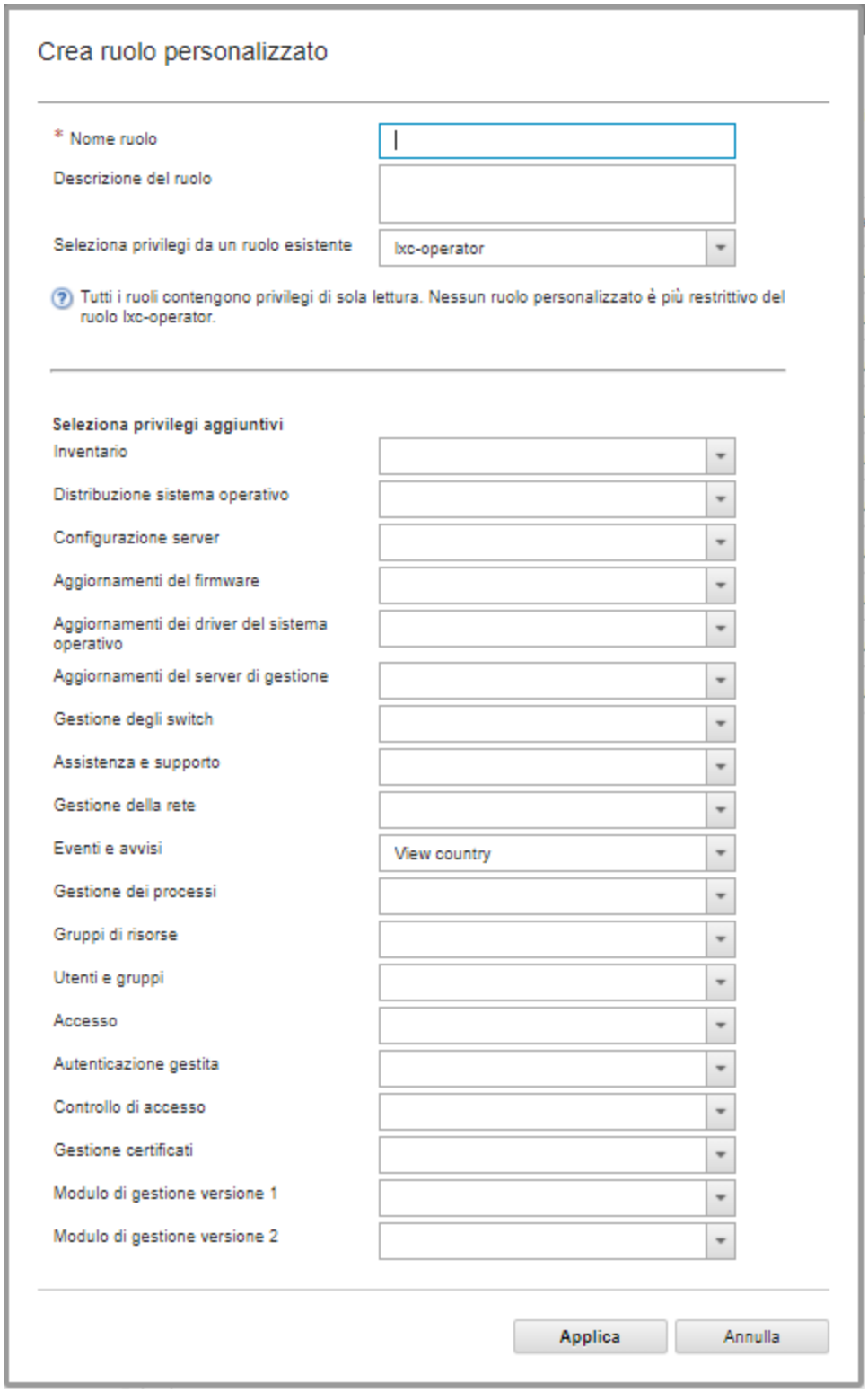
Per creare un ruolo personalizzato, effettuare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 2. Fare clic su **Ruoli** nella sezione "Utenti e gruppi" per visualizzare la pagina "Gestione ruoli".



Passo 3. Fare clic sull'icona **Crea** ( ) per creare un ruolo. Viene visualizzata la finestra di dialogo Crea ruolo personalizzato.



Passo 4. Immettere il nome del ruolo e la descrizione.

Passo 5. Selezionare un ruolo predefinito da utilizzare come punto di partenza per questo ruolo personalizzato.

Se si seleziona un ruolo esistente, i privilegi associati a questo ruolo vengono selezionati nella finestra di dialogo.

Passo 6. Modificare i privilegi per questo ruolo nuovo selezionando o cancellando i privilegi dal menu a discesa **Seleziona privilegi aggiuntivi**.

Nota: Se si selezionano tutti i privilegi in una categoria specifica e i privilegi vengono aggiunti a tale categoria quando si aggiorna XClarity Administrator, i nuovi privilegi vengono aggiunti automaticamente al ruolo personalizzato

Passo 7. Fare clic su **Crea**. Il nuovo ruolo viene aggiunto alla tabella nella pagina "Gestione ruoli".

Risultati

È inoltre possibile completare le seguenti azioni.

- Visualizzare i privilegi associati a un ruolo specifico selezionando il ruolo e facendo clic sull'icona **Visualizza** ( ).
- Rinominare o modificare il ruolo personalizzato facendo clic sull'icona **Modifica** ( ). Quando si modifica un ruolo personalizzato, è possibile modificare i privilegi selezionati, la descrizione e l'elenco degli utenti associati al ruolo.

  Nota: Non è possibile modificare un ruolo predefinito
- Eliminare il ruolo predefinito o personalizzato facendo clic sull'icona **Elimina** ( ).
- Aggiungere o rimuovere i ruoli da un gruppo di ruoli (vedere Aggiunta e rimozione di più utenti da un gruppo di ruoli).
- Ripristinare tutti i ruoli predefiniti eliminati facendo clic su **Tutte le azioni → Ripristina ruoli predefiniti**.

Privilegi predefiniti

Lenovo XClarity Administrator fornisce una serie di *privilegi* (autorizzazioni) che consentono all'utente di eseguire un'azione specifica. I privilegi sono organizzati in categorie in base al tipo di azione.

Privilegi di accesso

Questi privilegi forniscono le autorizzazioni per modificare le modalità di crittografia e SSL/TLS.

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-sec-apply-crypto-settings	Applicazione delle impostazioni di crittografia	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegi di controllo degli accessi

Questi privilegi forniscono le autorizzazioni per controllare l'accesso alle risorse.

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-sec-modify-resource-access-control	Modifica delle impostazioni di controllo di accesso alle risorse	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegi di gestione dei certificati

Questi privilegi forniscono le autorizzazioni per gestire i certificati di sicurezza in Lenovo XClarity Administrator.

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-sec-add-external-certificates	Aggiunta di un certificato esterno	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-add-trusted-certificates	Aggiunta di un certificato attendibile	lxc-recovery, lxc-security-admin, lxc-supervisor

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-sec-certificate-signing	Generazione della richiesta di firma del certificato	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-external-certificates	Eliminazione di un certificato esterno esistente	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-trusted-certificates	Eliminazione di un certificato esistente	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-ca	Download del certificato radice autorità di certificazione	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-server-certificate	Download del certificato server	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-certificate-revocation-list	Modifica o sostituzione dell'elenco di revoche di certificati	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-ca	Rigenerazione di un certificato radice autorità di certificazione	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-download-ca	Rigenerazione di un certificato radice autorità di certificazione	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-server-certificate	Rigenerazione del certificato server	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-resolve-untrusted-certificates	Risoluzione dei certificati non attendibili	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-upload-server-certificate	Caricamento del certificato server	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_view_certpol_settings	Visualizzazione delle impostazioni dei criteri	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_apply_certpol_settings	Applicazione delle impostazioni dei criteri	lxc-security-admin, lxc-supervisor

Privilegi di monitoraggio ed eventi

Questi privilegi forniscono le autorizzazioni per gestire eventi e avvisi.

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-event-audit	Gestione di log eventi e di controllo	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-create-edit-event-forwarders	Creazione e modifica dei server d'inoltro degli eventi	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-monitoring-create-edit-push-services	Creazione e modifica dei servizi push	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-event-forwarders	Eliminazione dei server d'inoltro degli eventi	lxc-admin, lxc-hw-admin, lxc-supervisor

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-monitoring-remove-push-services	Eliminazione dei servizi push	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-set-event-thresholds	Impostazione soglie eventi	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilegi degli aggiornamenti firmware

Questi privilegi forniscono le autorizzazioni per gestire e applicare gli aggiornamenti firmware e i pacchetti UpdateXpress System Packs.

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-fwUpdates-apply-assign-policy	Assegnazione dei criteri di conformità del firmware ai dispositivi	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-apply-perform-updates	Operazione di aggiornamento firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-create-policies	Creazione, copia, modifica e importazione dei criteri di conformità del firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-delete-policies	Eliminazione dei criteri di conformità	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-delete-packages	Eliminazione dei pacchetti di aggiornamento firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-download-packages	Download e importazione di pacchetti di aggiornamento firmware e aggiornamento del catalogo dei pacchetti di aggiornamento firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-export-packages	Esportazione dei pacchetti di aggiornamento firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor

Privilegi dei gruppi di risorse

Questi privilegi forniscono le autorizzazioni per utilizzare i gruppi di risorse.

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-resource-create-edit-group	Creazione e modifica di gruppi di risorse	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-resource-delete-group	Eliminazione di gruppi di risorse	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegi di inventario

Questi privilegi forniscono le autorizzazioni per rilevare e gestire i dispositivi e visualizzare l'inventario dei dispositivo.

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-dm-manage-device	Gestione di chassis, server, storage e switch.	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-dm-modify-ip-settings	Abilitazione o disabilitazione del controllo degli indirizzi IP duplicati nella stessa sottorete	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-inventory-modify-device-power-state	Modifica di canister, CMM, nodi, storage e stato di alimentazione degli switch	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-properties	Modifica di cabinet, canister, chassis, CMM, nodi, storage e proprietà degli switch	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-node-pfa-config-settings	Modifica delle impostazioni di configurazione PFA (Predicted Failure Alert)	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Privilegi di gestione dei processi

Questi privilegi forniscono le autorizzazioni per gestire i processi (attività).

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-tasks-remove-jobs	Eliminazione dei processi	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-tasks-schedule-jobs	Pianificazione dei processi	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilegi di autenticazione gestiti

Questi privilegi forniscono le autorizzazioni per gestire l'autenticazione, incluse le credenziali memorizzate.

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-sec-delete-stored-credentials	Eliminazione delle credenziali memorizzate	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-stored-credentials	Modifica delle credenziali memorizzate esistenti	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegi del modulo di gestione v1

Questi privilegi sono associati ai bit di autorizzazione LDAP (bitstring) applicati dai moduli di gestione per i server rack e per l'intero chassis di Flex System (inclusi tutti i dispositivi nello chassis).

Lenovo XClarity Administrator non applica queste autorizzazioni. Le autorizzazioni vengono applicate dai dispositivi gestiti che utilizzano un account XClarity Administrator.

Se il dispositivo viene gestito utilizzando l'*autenticazione gestita* (mediante il server di autenticazione locale per l'autenticazione), il server di autenticazione locale usa queste autorizzazioni per indicare ai dispositivi gestiti le autorizzazioni da concedere all'utente quando esegue il login al dispositivo.

Configurare le stesse autorizzazioni in un server LDAP esterno. Quando si utilizza un server LDAP esterno con XClarity Administrator, accertarsi di aggiungere gruppi a tale server con nomi che corrispondano ai nomi dei gruppi dei ruoli in XClarity Administrator e che gli utenti LDAP esterni vengano inseriti in uno o più di questi gruppi. Gli utenti LDAP esterni devono far parte di un gruppo LDAP con un nome corrispondente a un gruppo di ruoli XClarity Administrator contenente i ruoli associati alle stringhe di bit del modulo di gestione. XClarity Administrator utilizza questi gruppi per collegare gli utenti LDAP esterni ai gruppi di ruoli in XClarity Administrator e alle stringhe di bit applicate dal modulo di gestione. Quando quindi un utente esegue il login a un dispositivo gestito utilizzando un account utente LDAP esterno, il modulo di gestione sa se concedere i privilegi di supervisore utente o operatore.

Nota: I privilegi del modulo di gestione v1 non sono supportati per gli switch FlexSystem per i quali Secure IOM non è abilitato, gli switch RackSwitch, i dispositivi di storage e i server ThinkServer.

Per informazioni sui bit di autorizzazione LDAP per ciascun modulo di gestione, consultare la documentazione online.

- Configurazione di LDAP nella documentazione online dei moduli CMM e CMM2
- Configurazione di LDAP nella documentazione online dei moduli IMM e IMM2
- Configurazione di LDAP nella documentazione online di XCC

Nome privilegio	Descrizione privilegio	ruoli predefiniti
mm-advanced-adaptor-configuration-v1	Configurazione avanzata dell'adattatore	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-basic-configuration-v1	Configurazione base	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-clear-event-logs-v1	Cancellazione dei log eventi	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v1	Nega sempre	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-networking-and-security-v1	Rete e sicurezza	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-power-and-restart-access-v1	Alimentazione/riavvio/accesso per server e switch Flex	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-access-v1	Accesso al controllo remoto per i server	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-and-virtual-media-access-v1	Accesso alla console remota e ai supporti virtuali per i server	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-supervisor-v1	Accesso da supervisore	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-user-account-management-v1	Gestione utenti	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegi del modulo di gestione v2

Questi privilegi sono associati ai bit di autorizzazione LDAP (bitstring) applicati dai moduli di gestione per i singoli dispositivi FlexSystem e ThinkSystem in uno chassis (chassis, server e switch per i quali Secure IOM è abilitato).

Lenovo XClarity Administrator non applica queste autorizzazioni. Le autorizzazioni vengono applicate dai dispositivi gestiti che utilizzano un account XClarity Administrator.

Se il dispositivo viene gestito utilizzando l'*autenticazione gestita* (mediante il server di autenticazione locale per l'autenticazione), il server di autenticazione locale usa queste autorizzazioni per indicare ai dispositivi gestiti le autorizzazioni da concedere all'utente quando esegue il login al dispositivo.

Configurare le stesse autorizzazioni in un server LDAP esterno. Quando si utilizza un server LDAP esterno con XClarity Administrator, accertarsi di aggiungere gruppi a tale server con nomi che corrispondano ai nomi dei gruppi dei ruoli in XClarity Administrator e che gli utenti LDAP esterni vengano inseriti in uno o più di questi gruppi. Gli utenti LDAP esterni devono far parte di un gruppo LDAP con un nome corrispondente a un

gruppo di ruoli XClarity Administrator contenente i ruoli associati alle stringhe di bit del modulo di gestione. XClarity Administrator utilizza questi gruppi per collegare gli utenti LDAP esterni ai gruppi di ruoli in XClarity Administrator e alle stringhe di bit applicate dal modulo di gestione. Quando quindi un utente esegue il login a un dispositivo gestito utilizzando un account utente LDAP esterno, il modulo di gestione sa se concedere i privilegi di supervisore utente o operatore.

Nota:

- È inoltre necessario specificare i privilegi del modulo di gestione v1 per l'intero chassis (vedere Privilegi del modulo di gestione v1).
- I privilegi di del modulo di gestione v2 non sono supportati per gli switch FlexSystem per i quali Secure IOM non è abilitato.
- Per lo chassis Lenovo ThinkSystem, accertarsi che IMM2 sia configurato in modo da consentire l'"amministrazione del nodo" al ruolo personalizzato. Se si desidera che il ruolo personalizzato abbia il controllo di tutti i dispositivi nello chassis Lenovo ThinkSystem, accertarsi che IMM2 sia configurato in modo da consentire anche al ruolo personalizzato di disporre dell'"ambito Node X".

Per informazioni sui bit di autorizzazione LDAP per ciascun modulo di gestione, consultare la documentazione online.
- Configurazione di LDAP nella documentazione online dei moduli CMM e CMM2
- Configurazione di LDAP nella documentazione online dei moduli IMM e IMM2
- Configurazione di LDAP nella documentazione online di XCC

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
mm-blade-1-scope-v2	Ambito nodo 1	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-2-scope-v2	Ambito nodo 2	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-3-scope-v2	Ambito nodo 3	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-4-scope-v2	Ambito nodo 4	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-5-scope-v2	Ambito nodo 5	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-6-scope-v2	Ambito nodo 6	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-7-scope-v2	Ambito nodo 7	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-8-scope-v2	Ambito nodo 8	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-9-scope-v2	Ambito nodo 9	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-10-scope-v2	Ambito nodo 10	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-11-scope-v2	Ambito nodo 11	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-12-scope-v2	Ambito nodo 12	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
mm-blade-13-scope-v2	Ambito nodo 13	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-14-scope-v2	Ambito nodo 14	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-administration-v2	Amministrazione del nodo	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-configuration-v2	Configurazione del nodo	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-operator-v2	Operatore blade	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-remote-presence-v2	Presenza remota del nodo	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-administration-v2	Amministrazione dello chassis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-configuration-v2	Configurazione dello chassis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-log-management-v2	Gestione dell'account di log dello chassis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-operator-v2	Operatore chassis	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-chassis-scope-v2	Ambito chassis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-user-account-management-v2	Gestione utenti	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v2	Nega sempre	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-io-module-1-scope-v2	Ambito modulo I/O 1	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-2-scope-v2	Ambito modulo I/O 2	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-3-scope-v2	Ambito modulo I/O 3	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-4-scope-v2	Ambito modulo I/O 4	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-administration-v2	Amministrazione switch	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-configuration-v2	Configurazione switch	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
mm-switch-operator-v2	Operatore switch	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-supervisor-v2	Accesso da supervisore	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilegi dei server di gestione

Questi privilegi forniscono le autorizzazioni per aggiornare il server di gestione.

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-mgmtserverupdates-delete-updates	Eliminazione degli aggiornamenti del server di gestione	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-download-updates	Download e importazione degli aggiornamenti del server di gestione e aggiornamento del catalogo dei server di gestione	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-perform-updates	Esecuzione degli aggiornamenti del server di gestione	lxc-admin, lxc-fw-admin, lxc-supervisor

Privilegi di gestione della rete

Questi privilegi forniscono le autorizzazioni per configurare le impostazioni di rete.

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-network-edit	Modifica dell'accesso alla rete	lxc-admin, lxc-supervisor

Privilegi di distribuzione sistema operativo

Questi privilegi forniscono le autorizzazioni per distribuire i sistemi operativi.

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-osdeploy-create-edit-remote-file-server	Creazione e modifica di una voce del file server remoto	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-create-import-export-edit-os-files	Creazione, importazione, esportazione e modifica delle immagini del sistema operativo e dei file personalizzati	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-os-files	Eliminazione delle immagini del sistema operativo e dei file personalizzati	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-remote-file-server	Eliminazione di una voce del file server remoto	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-osdeploy-edit-global-settings	Modifica delle informazioni nella finestra di dialogo delle impostazioni globali **Nota:** La modifica delle impostazioni di assegnazione degli IP globali incide sulle impostazioni di rete; pertanto, per apportare modifiche alle impostazioni di assegnazione degli IP globali è necessario disporre dei privilegi **lxc-osdeploy-edit-settings-and-deploy-os-images**.	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-settings-and-deploy-os-images	Modifica delle impostazioni di distribuzione e distribuzione di immagini del sistema operativo a uno o più server	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilegi di aggiornamento dei driver del sistema operativo

Questi privilegi forniscono le autorizzazioni per gestire e applicare gli aggiornamenti dei driver di dispositivo del sistema operativo.

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-osDriverUpdates-apply-assign-uxsp	Assegnazione dei pacchetti UXSP dei driver di dispositivo del sistema operativo ai dispositivi	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-authentication	Controllo dell'autenticazione del sistema operativo	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-compliance	Controllo della conformità dei driver di dispositivo del sistema operativo	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-perform-updates	Esecuzione degli aggiornamenti dei driver di dispositivo del sistema operativo	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-delete-packages	Eliminazione dei pacchetti di aggiornamento dei driver di dispositivo del sistema operativo	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-download-packages	Download e importazione dei pacchetti di aggiornamento dei driver di dispositivo del sistema operativo e aggiornamento del catalogo UXSP dei driver di dispositivo del sistema operativo	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilegi di utenti e gruppi

Questi privilegi forniscono le autorizzazioni per gli account di utenti e gruppi.

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-sec-apply-saml-settings	Applicazione delle impostazioni SAML	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-role-groups	Eliminazione di un gruppo di ruoli	lxc-recovery, lxc-security-admin, lxc-supervisor

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-sec-delete-roles	Eliminazione di un ruolo	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-users	Eliminazione di un utente	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-edit-account-settings	Modifica delle impostazioni di sicurezza dell'account	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-ldap-settings	Applicazione delle impostazioni LDAP	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-role-groups	Modifica di un gruppo di ruoli	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-roles	Modifica di un ruolo	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-users	Modifica di un utente	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilegi di configurazione server

Questi privilegi forniscono le autorizzazioni per eseguire il provisioning o il preprovisioning dei server mediante i pattern di configurazione.

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-cp-edit-management-ip	Modifica degli indirizzi IP di gestione per lo chassis	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-edit-preferences	Impostazione delle preferenze dei pattern di configurazione	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-address-pools	Gestione dei pool di indirizzi	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-patterns	Gestione dei pattern	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-placeholders	Gestione degli segnaposti	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-profiles	Distribuzione di pattern e segnaposto agli chassis e gestione dei profili	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-other-server-config	Reimpostazione dello storage locale e applicazione dell'operazione di sicurezza Intel Optane DCPMM	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilegi dei servizi

Questi privilegi forniscono le autorizzazioni per definire i contatti di supporto per ciascun dispositivo gestito, raccogliere e inviare i file di servizio al supporto Lenovo, configurare le notifiche automatiche per i provider di servizi quando si verifica un evento che richiede assistenza per specifici dispositivi, visualizzare lo stato del ticket di assistenza e le informazioni sulla garanzia e raccogliere e inviare i dati di servizio.

Nome privilegio	Descrizione privilegio	Ruoli predefiniti
lxc-ss-alter-backup-credentials	Modifica delle credenziali FFDC di backup	lxc-admin, lxc-hw-admin, lxc-service-admin, lxc-supervisor
lxc-ss-call-home	Esecuzione di Call Home	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-recovery-password	Modifica password di ripristino del servizio	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-tickets	Modifica dei ticket di assistenza	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-remove-service-tickets	Eliminazione dei ticket di assistenza	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-run-service-forwarders	Esecuzione dei server d'inoltro di servizio	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilegi di configurazione degli switch

Questi privilegi forniscono le autorizzazioni per configurare gli switch ed eseguire il backup e il ripristino dei dati di configurazione degli switch.

Nome privilegio	Descrizione privilegio	ruoli predefiniti
lxc-netcfg-template-management	Creazione, modifica, eliminazione e distribuzione dei modelli di configurazione degli switch ed eliminazione di una distribuzione della configurazione degli switch	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-config-management	Backup, ripristino, eliminazione, esportazione e importazione dei file dei dati di configurazione degli switch	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-port-management	Modifica dello stato delle porte degli switch	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Creazione di un gruppo di ruoli personalizzato

Un *gruppo di ruoli* è un insieme di ruoli e di utenti membri dello stesso insieme di ruoli. Il livello di accesso concesso a ciascun utente nel gruppo di ruoli è basato su ruoli assegnati a questo gruppo di ruoli. XClarity Administrator fornisce le seguenti operazioni predefiniti gruppi di ruoli, che corrispondono ai ciascuno dei ruoli predefiniti. È inoltre possibile creare gruppi di ruoli personalizzati.

Informazioni su questa attività

Ogni utente XClarity Administrator deve essere membro di almeno un gruppo di ruoli.

I seguenti gruppi di ruoli sono predefiniti in XClarity Administrator.

- **LXC-SUPERVISOR**. Include il ruolo **lxc-supervisor**.
- **LXC-ADMIN**. Include il ruolo **lxca-admin**.
- **LXC-SECURITY-ADMIN**. Include il ruolo **lxc-security-admin**.
- **LXC-HW-ADMIN**. Include il ruolo **lxc-hw-admin**.
- **LXC-FW-ADMIN**. Include il ruolo **lxc-fw-admin**.
- **LXC-OS-ADMIN**. Include il ruolo **lxc-os-admin**.

- **LXC-SERVICE-ADMIN**. Include il ruolo **lxc-service-admin**.
- **LXC-HW-MANAGER**. Include il ruolo **lxc-hw-manager**.
- **LXC-OPERATOR**. Include il ruolo **lxc-operator**.
- **LXC-RECOVERY**. Include il ruolo **lxc-recovery**.

I seguenti ruoli predefiniti sono *riservati* e non possono essere utilizzati per creare nuovi gruppi di ruoli o assegnati a nuovi utenti.
- **lxc-sysrdr**
- **lxc-sysmgr**

Procedura

Per creare un gruppo di ruoli, effettuare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 2. Fare clic su **Gruppi di ruoli** nella sezione "Utenti e gruppi" per visualizzare la pagina "Gestione gruppi".

Passo 3. Fare clic sull'icona **Crea** ( ) per creare un gruppo di ruoli. Viene visualizzata la finestra di dialogo Crea nuovo gruppo di ruoli.

Passo 4. Immettere il nome del gruppo e la descrizione.

Nota: Suggerimento: per il nome del gruppo è possibile utilizzare lettere, numeri, spazi, caratteri di sottolineatura, trattini e punti.

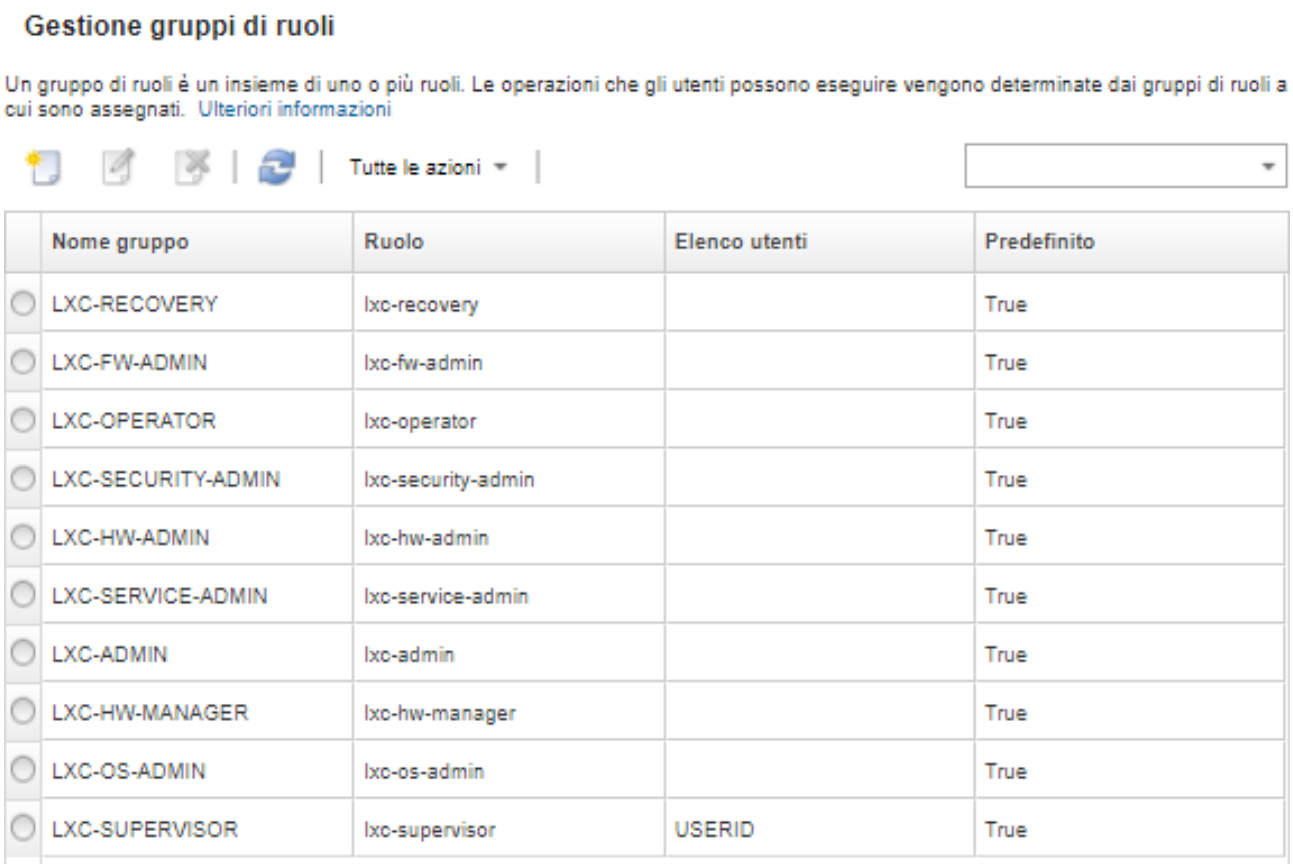
Passo 5. Selezionare uno o più ruoli da assegnare a questo gruppo di ruoli.

Passo 6. Selezionare uno o più utenti membri di questo gruppo di ruoli.

Passo 7. Fare clic su **Crea**. Il nuovo gruppo di ruoli viene aggiunto alla tabella nella pagina "Gestione gruppo".

Risultati

Il gruppo di ruoli viene visualizzato nella tabella "Gruppi di ruoli". La tabella mostra i ruoli di autorizzazione associati e i membri di ogni gruppo di ruoli.



Dopo aver creato un gruppo di ruoli, è possibile eseguire le seguenti azioni su un gruppo di ruoli selezionato:

- Aggiungere o rimuovere i ruoli assegnati a questo gruppo di ruoli facendo clic sull'icona **Modifica** ( ).
- Aggiungere o rimuovere gli utenti come membri del gruppo di ruoli (vedere "Aggiunta e rimozione di più utenti da un gruppo di ruoli" a pagina 57).
- Esportare le informazioni sui gruppi di ruoli, incluse le autorizzazioni di accesso, facendo clic su **Tutte le azioni → Esporta come CSV**.
- Eliminare il gruppo di ruoli facendo clic sull'icona **Elimina** ( ).È possibile eliminare i gruppi di ruoli predefiniti.

Una volta creato, modificato o eliminato un gruppo di ruoli, la modifica viene fornita immediatamente a ogni dispositivo gestito.

Aggiunta e rimozione di più utenti da un gruppo di ruoli

È possibile modificare l'appartenenza a un gruppo di ruoli aggiungendo o rimuovendo più utenti.

Procedura

Completare le seguenti operazioni per aggiungere e rimuovere gli utenti da un gruppo di ruoli.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 2. Fare clic su **Gruppi di ruoli** nella sezione "Utenti e gruppi" per visualizzare la pagina "Gestione gruppi".

Passo 3. Fare clic sull'icona **Modifica** ( ) per modificare il gruppo di ruoli. Viene visualizzata la finestra di dialogo Modifica gruppo di ruoli.

Passo 4. Fare clic sull'elenco a discesa **Elenco utenti** e selezionare gli utenti da includere o cancellare l'utente per escluderlo da questo gruppo di ruoli.

Passo 5. Fare clic su **Salva**. Nella colonna **Elenco utenti** viene visualizzata l'appartenenza dell'utente corrente nel gruppo di ruoli.

Gestione dell'accesso ai dispositivi

Il controllo dell'accesso ai dispositivi è disabilitato per impostazione predefinita e non viene reso effettivo finché non è abilitato

Quando i dispositivi vengano gestiti inizialmente da Lenovo XClarity Administrator, una serie predefinita di gruppi di ruoli dispone dell'autorizzazione per accedere ai dispositivi per impostazione predefinita. Questa serie predefinita è vuota per impostazione predefinita, finché non viene configurata.

È possibile modificare i gruppi di ruoli che possono accedere a specifici dispositivi gestiti. Quando l'autorizzazione è assegnata a determinati gruppi di ruoli, solo gli utenti membri di questi gruppi di ruoli possono visualizzare e utilizzare questi dispositivi specifici.

Controllo dell'accesso a dispositivi specifici

Quando i dispositivi vengano gestiti inizialmente da Lenovo XClarity Administrator, una serie predefinita di gruppi di ruoli dispone dell'autorizzazione per accedere ai dispositivi per impostazione predefinita. È possibile modificare i gruppi di ruoli che possono accedere a specifici dispositivi gestiti. Quando l'autorizzazione è assegnata a determinati gruppi di ruoli, solo gli utenti membri di questi gruppi di ruoli possono visualizzare e utilizzare questi dispositivi specifici.

Prima di iniziare

Solo gli utenti con autorità **lxc-supervisor**, **lxc-security-admin** o **lxc-recovery** possono eseguire questa azione.

Informazioni su questa attività

Il controllo dell'accesso viene configurato sui singoli dispositivi. Non è impostato per i contenitori, come rack e i gruppi di risorse.

Per i componenti in uno chassis o in un enclosure, gli utenti devono disporre almeno dell'accesso di sola lettura allo chassis o all'enclosure per visualizzare i componenti di tale chassis o enclosure. Se gli utenti non dispongono almeno dell'accesso di sola lettura allo chassis o all'enclosure, potrebbe comunque essere possibile visualizzare i componenti dello chassis in alcune viste ma non in tutte.

Gli utenti con autorità **lxc-supervisor** possono visualizzare e modificare tutte le risorse, indipendentemente dal fatto che si trovino in un gruppo di ruoli che dispone dell'accesso specifico a tale risorsa. Non è possibile rimuovere l'accesso a qualsiasi risorsa per il gruppo di ruoli **lxc-supervisor**.

Se un utente non è membro di un gruppo di ruoli che dispone dell'accesso a un dispositivo gestito specifico, l'utente non può visualizzare o modificare tale dispositivo specifico. Ciò include l'avvio dell'interfaccia Web del controller di gestione tramite Lenovo XClarity Administrator. Inoltre, per i dispositivi Flex e System x, gli utenti non possono accedere direttamente a un modulo CMM o al controller di gestione a cui non sono autorizzati ad accedere.

Le impostazioni predefinite di controllo dell'accesso vengono utilizzate per impostare le autorizzazioni di accesso sui dispositivi, quando vengono gestiti inizialmente da XClarity Administrator e per ripristinare le impostazioni predefinite delle autorizzazioni di accesso per uno specifico dispositivo. La modifica delle

impostazioni predefinite di controllo dell'accesso non comporta la modifica automatica delle autorizzazioni di accesso sui dispositivi già gestiti.

Importante:

- Se un utente è membro di più gruppi di ruoli assegnati a diversi dispositivi, le azioni che l'utente è autorizzato a eseguire su ciascun dispositivo possono variare. Ad esempio, se l'utente è membro dei gruppi di ruoli predefiniti LXC-FW-ADMIN e LXC-OS-ADMIN ma solo LXC-FW-ADMIN può accedere al Server A, l'utente può aggiornare il firmware del Server A ma non può distribuire un sistema operativo sul Server A. Se invece solo LXC-OS-ADMIN è autorizzato ad accedere al Server B, l'utente può distribuire un sistema operativo sul Server B, ma non può aggiornare il firmware del Server B.
- Quando si limita l'accesso a un dispositivo dotato di una risorsa principale (come un server o uno switch in uno chassis Flex), un utente deve disporre almeno delle autorizzazioni di sola lettura alla risorsa principale per interagire in modo completo con il dispositivo. Se un utente dispone almeno dell'accesso in sola lettura al dispositivo, ma non alla risorsa principale, l'utente non potrà visualizzare le viste dell'inventario del dispositivo, ma potrebbe accedere a informazioni sul dispositivo, come processi ed eventi.

  Ad esempio, è possibile creare un gruppo di ruoli per la risorsa principale e assegnare questo gruppo di ruoli al ruolo **lxc-operator**. Includere tutti gli utenti che devono accedere a qualsiasi risorsa secondaria (come un server o uno switch in uno chasis Flex), in questo gruppo di ruoli. Includere quindi questo gruppo di ruoli come uno dei gruppi che ha accesso alla risorsa principale.

Procedura

Attenersi alla seguente procedura per controllare l'accesso ai dispositivi specifici associando i gruppi di ruoli a tali dispositivi.

Passo 1. Dal menu principale di Lenovo XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 2. Fare clic su **Visualizzazione risorse** nel riquadro di navigazione sinistro. Viene visualizzata la pagina "Visualizzazione risorse".

È possibile ordinare le colonne della tabella per semplificare l'identificazione di dispositivi specifici. Inoltre, è possibile selezionare un tipo di dispositivo nel menu a discesa **Tipo di risorsa**, selezionare un gruppo di ruoli nel menu a discesa **Gruppi di ruoli**, selezionare un gruppo di risorse nel menu a discesa **Gruppi di risorse**e immettere il testo (ad esempio, nome o tipo di risorsa) nel campo **Filtro** per visualizzare solo l'elenco dei dispositivi che soddisfano i criteri selezionati.

Passo 3. Selezionare uno o più dispositivi di cui si desidera controllare l'accesso.

Passo 4. Fare clic sull'icona **Modifica** ( ). Viene visualizzata la finestra di dialogo "Modifica risorsa" con i dispositivi di destinazione selezionati, elencati nel campo **Nome risorsa**.

Passo 5. Dall'elenco a discesa **Gruppi di ruoli**, selezionare i gruppi di ruoli a cui si desidera concedere l'accesso ai dispositivi di destinazione.

Nota: Se il dispositivo è dotato di una risorsa principale (come un server o uno switch in uno chassis Flex), è possibile specificare l'accesso sia al dispositivo (colonna destra) sia alla risorsa principale (colonna sinistra).

Passo 6. Configurare **Accesso pubblico** su `No`. Ciò significa che solo gli utenti membri dei gruppi di ruoli selezionati possono accedere ai dispositivi di destinazione.

Passo 7. Fare clic su **Salva**.

Passo 8. Una volta completata l'assegnazione delle autorizzazioni, fare clic sull'interruttore **Disabilitato** per modificare il **Controllo accesso alla risorsa** in "Abilitato".

È possibile abilitare il controllo dell'accesso alla risorsa in qualsiasi momento, prima o dopo la configurazione dell'accesso ai dispositivi specifici. Se questa impostazione è abilitata, la

configurazione visualizzata nella tabella viene applicata, incluso il rifiuto dell'accesso degli utenti non supervisori per tutti i dispositivi che non dispongono di alcun gruppo configurato per accedervi.

Al termine

È anche possibile controllare l'accesso ai dispositivi eseguendo le seguenti azioni:

- Per modificare le autorizzazioni per i gruppi di ruoli predefiniti e l'impostazione di accesso pubblico, fare clic sull'icona **Modifica** () e quindi su **Ripristina valori predefiniti**.
- Modificare il gruppo di ruoli predefinito e l'impostazione di accesso pubblico (vedere Modifica delle autorizzazioni predefinite.).
- Disabilitare il controllo dell'accesso alla risorsa facendo clic sull'interruttore **Abilitato** per modificare **Controllo accesso alla risorsa** in "Disabilitato". In questo modo, tutti i gruppi di ruoli possono accedere a tutti i dispositivi gestiti.

Disabilitazione del controllo di accesso alla risorsa

Viene disabilitato il controllo dell'accesso per tutti i dispositivi o per dispositivi specifici, in modo che tutti gli utenti possano visualizzare e utilizzare questi dispositivi.

Informazioni su questa attività

Solo gli utenti con autorità **lxc-supervisor**, **lxc-security-admin** o **lxc-recovery** possono eseguire questa azione.

Procedura

Completare le seguenti operazioni per disabilitare il controllo dell'accesso alla risorsa.

- Per tutti i dispositivi gestiti
  1. Dal menu principale di Lenovo XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
  2. Fare clic su **Visualizzazione risorse** nel riquadro di navigazione sinistro. Viene visualizzata la pagina "Visualizzazione risorse".
  3. Fare clic sull'interruttore **Abilitato** per modificare il **Controllo accesso alla risorsa** in "Disabilitato".
- Per dispositivi gestiti specifici
  1. Dal menu principale di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.
  2. Fare clic su **Visualizzazione risorse** nel riquadro di navigazione sinistro. Viene visualizzata la pagina "Visualizzazione risorse".

     È possibile ordinare le colonne della tabella per semplificare l'identificazione di dispositivi specifici. Inoltre, è possibile selezionare un tipo di dispositivo nel menu a discesa **Tipo di risorsa**, selezionare un gruppo di ruoli nel menu a discesa **Gruppi di ruoli**, selezionare un gruppo di risorse nel menu a discesa **Gruppi di risorse** e immettere il testo (ad esempio, nome o tipo di risorsa) nel campo **Filtro** per visualizzare solo l'elenco dei dispositivi che soddisfano i criteri selezionati.
  3. Selezionare uno o più dispositivi per cui si desidera modificare l'accesso.
  4. Fare clic sull'icona **Modifica** (). Viene visualizzata la finestra di dialogo "Modifica risorsa" con i dispositivi selezionati elencati nel campo **Nome risorsa**.
  5. Configurare **Accesso pubblico** su `Yes`. Ciò significa che tutti i gruppi di ruoli possono accedere ai dispositivi di destinazione indipendentemente dai gruppi di ruoli elencati nell'elenco a discesa **Gruppi di ruoli**.
  6. Fare clic su **Salva**.

Modifica delle autorizzazioni predefinite

Sono disponibili due impostazioni che determinano se i gruppi di ruoli possono accedere ai dispositivi, quando vengono gestiti inizialmente da Lenovo XClarity Administrator: accesso pubblico e gruppi di ruoli. L'impostazione di accesso pubblico determina se tutti o una serie specifica di gruppi di ruoli può accedere ai dispositivi di destinazione. Per impostazione predefinita, questa opzione è configurata su `Yes`; ciò significa che tutti i gruppi di ruoli possono accedere ai dispositivi di destinazione. È possibile modificare il comportamento predefinito configurando l'impostazione di accesso pubblico su `No` e quindi selezionando la serie di gruppi di ruoli che possono accedere ai dispositivi di destinazione

Informazioni su questa attività

Solo gli utenti con autorità **lxc-supervisor**, **lxc-security-admin** o **lxc-recovery** possono eseguire questa azione.

Gli utenti con autorità **lxc-supervisor**, **lxc-security-admin** o **lxc-recovery** possono accedere a tutti i dispositivi gestiti. Non è possibile rimuovere l'accesso a qualsiasi dispositivo per questi gruppi di ruoli.

Le impostazioni predefinite di controllo dell'accesso vengono utilizzate per impostare le autorizzazioni di accesso sui dispositivi, quando vengono gestiti inizialmente da XClarity Administrator e per ripristinare le impostazioni predefinite delle autorizzazioni di accesso per uno specifico dispositivo. La modifica delle impostazioni predefinite di controllo dell'accesso non comporta la modifica automatica delle autorizzazioni di accesso sui dispositivi già gestiti.

Procedura

Completare la seguente procedura per modificare i controlli di accesso predefiniti.

Passo 1. Dal menu principale di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 2. Fare clic su **Visualizzazione risorse** nel riquadro di navigazione sinistro. Viene visualizzata la pagina "Visualizzazione risorse".

È possibile ordinare le colonne della tabella per semplificare l'identificazione di dispositivi specifici. Inoltre, è possibile selezionare un tipo di dispositivo nel menu a discesa **Tipo di risorsa**, selezionare un gruppo di ruoli nel menu a discesa **Gruppi di ruoli**, selezionare un gruppo di risorse nel menu a discesa **Gruppi di risorse**e immettere il testo (ad esempio, nome o tipo di risorsa) nel campo **Filtro** per visualizzare solo l'elenco dei dispositivi che soddisfano i criteri selezionati.

Passo 3. Fare clic su **Tutte le azioni → Modifica risorse predefinite**. Viene visualizzata la finestra di dialogo "Modifica risorse predefinite".

Passo 4. Dall'elenco a discesa **Gruppi di ruoli**, selezionare i gruppi di ruoli che si desidera definire come serie predefinita.

Passo 5. Selezionare l'impostazione predefinita **Accesso pubblico**.

- **Sì**. Quando un dispositivo viene gestito inizialmente, tutti i gruppi di ruoli possono accedere a tale dispositivo, indipendentemente dai gruppi di ruoli elencati nell'elenco a discesa **Gruppi di ruoli**.
- **No**. Quando un dispositivo viene gestito inizialmente, solo i gruppi di ruoli elencati nell'elenco a discesa **Gruppi di ruoli** possono accedere a tale dispositivo per impostazione predefinita.

Passo 6. Fare clic su **Salva**.

Implementazione di un ambiente sicuro

È importante valutate i requisiti di sicurezza dell'ambiente, comprendere e ridurre tutti i rischi per la sicurezza. Lenovo XClarity Administrator include diverse funzioni che semplificano la protezione

dell'ambiente. Utilizzare le seguenti informazioni per facilitare l'implementazione di un piano di sicurezza per l'ambiente.

Informazioni su questa attività

Importante: L'utente è responsabile di valutazione, scelta e implementazione delle funzioni di sicurezza, delle procedure amministrative e dei controlli appropriati per l'ambiente del sistema. L'implementazione delle funzioni di sicurezza descritte in questa sezione non garantisce la protezione completa dell'ambiente.

Tenere presente le seguenti informazioni quando si valutano i requisiti di sicurezza dell'ambiente:

- La sicurezza fisica dell'ambiente è importante; limitare l'accesso alle sale e ai rack dove risiede l'hardware di gestione dei sistemi.
- Utilizzare un firewall software per proteggere i dati e l'hardware di rete da minacce per la sicurezza note ed emergenti, come virus e accessi non autorizzati.
- Non modificare le impostazioni di sicurezza predefinite degli switch di rete e i moduli pass-thru. Le impostazioni predefinite di fabbrica di questi componenti disabilitano l'uso dei protocolli non sicuri e abilitano il requisito di aggiornamenti firmware firmati.
- Le applicazioni di gestione di moduli CMM, controller di gestione della scheda di base, FSP e switch consentono solo pacchetti firmati di aggiornamento firmware per questi componenti, in modo da garantire l'installazione solo di firmware attendibili.
- Solo gli utenti autorizzati ad aggiornare i componenti del firmware devono disporre dell'autorità di aggiornamento firmware.
- È necessario garantire almeno l'installazione degli aggiornamenti firmware critici. Dopo avere apportato eventuali modifiche, eseguire sempre il backup della configurazione.
- Verificare che tutti gli aggiornamenti relativi alla sicurezza dei server DNS siano prontamente installati e aggiornati.
- Avvisare gli utenti di non accettare i certificati non attendibili. Per ulteriori informazioni, vedere Utilizzo dei certificati di sicurezza.
- L'hardware Flex System dispone di opzioni anti-manomissione. Se l'hardware è installato in un rack sbloccato o si trova in un'area aperta, installare le opzioni anti-manomissione per evitare e identificare le intrusioni. Per ulteriori informazioni sulle opzioni anti-manomissione, consultare la documentazione fornita con i prodotti Flex System.
- Se possibile, collocare l'hardware di gestione dei sistemi in una sottorete separata. In genere, solo gli amministratori devono avere accesso all'hardware di gestione dei sistemi.
- Quando si scelgono le password, non utilizzare espressioni facili da indovinare, come "password" o il nome della propria azienda. Conservare le password in un luogo sicuro e accertarsi che l'accesso alle password sia limitato. Implementare i criteri per le password definiti dall'azienda.

  Importante: Modificare sempre il nome utente e la password predefiniti. Tutti gli utenti devono rispettare le regole delle password sicure.
- Stabilire le password di accensione per gli utenti come metodo di controllo per chi accede a dati e programmi di installazione sui server. Per ulteriori informazioni sulle password di accensione, consultare la documentazione fornita con i server.
- Utilizzare i vari livelli di autorizzazione disponibili per gli utenti differenti dell'ambiente. Non consentire a tutti gli utenti di utilizzare lo stesso ID utente supervisore.
- Per supportare le comunicazioni sicure, verificare che l'ambiente risponda ai seguenti criteri NIST 800-131A:
  - Utilizzare Secure Sockets Layer (SSL) sul protocollo TLS v1.2.

- Utilizzare le funzioni di hash SHA-256 o più avanzate per le firme digitali e le funzioni di hash SHA-1 o più avanzate per le altre applicazioni.
- Utilizzare RSA-2048 o un metodo di crittografia ancora più sicuro oppure utilizzare la crittografia ECC (Elliptic Curve Cryptography) del NIST a 224 bit o superiore.
- Utilizzare la crittografia simmetrica approvata dal NIST con lunghezza delle chiavi di almeno 128 bit.
- Utilizzare i generatori di numeri casuali approvati dal NIST.
- Laddove possibile, supportare i meccanismi di scambio delle chiavi Diffie-Hellman o Elliptic Curve Diffie-Hellman.

Per ulteriori informazioni sulle impostazioni di crittografia, vedere Configurazione delle impostazioni di crittografia sul server di gestione. Per ulteriori informazioni sulle impostazioni NIST, vedere Implementazione della conformità NIST SP 800-131A.

Modifica delle impostazioni di sicurezza dell'account utente

Le impostazioni di sicurezza dell'account utente controllano la complessità della password, il blocco dell'account e il timeout di inattività della sessione Web. È possibile modificare i valori delle impostazioni.

Procedura

Completare le seguenti operazioni per sovrascrivere le impostazioni di sicurezza dell'account esistenti.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 2. Fare clic su **Impostazioni di sicurezza dell'account** nella sezione Utenti e gruppi per visualizzare la pagina Gestione utenti.

Passo 3. Per ognuna delle seguenti impostazioni da modificare, selezionare il nuovo valore.

Tabella 1. Impostazioni di sicurezza dell'account

Impostazioni di sicurezza	Descrizione	Valori consentiti	Valori predefiniti
Periodo di scadenza password	Intervallo di tempo (espresso in giorni) durante il quale un utente può utilizzare una password prima che sia tenuto a modificarla. Valori più piccoli riducono il periodo di tempo in cui gli utenti malintenzionati possono tentare di indovinare le password. Se il valore è impostato su **0**, le password non scadranno mai. **Nota:** Questa impostazione si applica solo quando gli account utente sono gestiti mediante il server di autenticazione locale. Non viene invece utilizzata quando si utilizza il server di autenticazione esterna.	**0 – 365**	**90**
Periodo di avviso scadenza password	Intervallo di tempo (espresso in giorni) precedente la data di scadenza della password durante il quale gli utenti ricevono avvisi relativi all'imminente scadenza della password. Se il valore è impostato su **0**, gli utenti non riceveranno mai avvisi. **Nota:** Questa impostazione si applica solo quando gli account utente sono gestiti mediante il server di autenticazione locale. Non viene invece utilizzata quando si utilizza il server di autenticazione esterna.	**0 -** *impostazione massima per la scadenza della password*	**5**

Tabella 1. Impostazioni di sicurezza dell'account (continua)

Impostazioni di sicurezza	Descrizione	Valori consentiti	Valori predefiniti
Ciclo minimo di riutilizzo password	Numero minimo di volte che un utente deve immettere una password univoca durante la modifica della password prima che l'utente possa iniziare a utilizzare nuovamente le password. Se il valore è impostato su **0**, gli utenti possono riutilizzare le password immediatamente.	**0 – 10**	**5**
Intervallo minimo di modifica password	Intervallo di tempo minimo (espresso in ore) che deve trascorrere prima che un utente possa modificare nuovamente una password già modificata in precedenza. Il valore specificato per questa impostazione non può superare il valore specificato per il periodo di scadenza della password. Se il valore è impostato su **0**, gli utenti possono modificare le password immediatamente.	**0 – 1440**	**24**
Numero massimo di errori di login	Numero massimo di volte che un utente può tentare di accedere con una password non corretta prima che l'account utente venga bloccato. Il numero specificato per il periodo di blocco in seguito al numero massimo di errori di login determina il periodo di tempo in cui l'account utente rimarrà bloccato. Gli account bloccati non possono essere utilizzati per accedere al sistema anche se viene immessa una password valida. Se il valore è impostato su **0**, gli account non vengono mai bloccati. Il contatore degli accessi non riusciti viene reimpostato su zero dopo un accesso riuscito.	**0 – 100**	**20**
Periodo di blocco in seguito al numero massimo di errori di login	Intervallo minimo di tempo (espresso in minuti) che deve trascorrere prima che un utente precedentemente bloccato possa provare nuovamente a eseguire il login. Se il valore è impostato su **0**, l'account rimane bloccato finché l'amministratore non lo sblocca esplicitamente. Se si imposta il valore 0, il sistema potrebbe essere esposto ad attacchi DoS (Denial of Service) in cui una serie di tentativi di login volutamente non validi può determinare il blocco permanente degli account. **Suggerimento:** qualsiasi utente con il ruolo di supervisore può sbloccare un account utente. Per ulteriori informazioni, vedere Sblocco di un utente. **Nota:** Questa impostazione si applica solo quando gli account utente sono gestiti mediante il server di autenticazione locale. Non viene invece utilizzata quando si utilizza il server di autenticazione esterna.	**0 – 2880**	**60**

Tabella 1. Impostazioni di sicurezza dell'account (continua)

Impostazioni di sicurezza	Descrizione	Valori consentiti	Valori predefiniti
Timeout sessione di inattività Web	Intervallo di tempo (espresso in minuti) durante il quale una sessione utente stabilita con XClarity Administrator può rimanere inattiva prima che l'utente venga scollegato. Se il valore è impostato su **0**, la sessione Web non scade mai. **Nota:** La modifica di questo valore è effettiva solo per le sessioni utente avviate dopo il cambiamento dell'impostazione.	**0 – 1440**	**1440**
Lunghezza minima password	Il numero minimo di caratteri che possono essere utilizzati per specificare una password valida.	**8 – 20**	**8**
Numero di regole di complessità che devono essere seguite durante la creazione di una nuova password.	Numero di regole di complessità che devono essere seguite durante la creazione di una nuova password. Le regole vengono applicate a partire dalla regola 1 e fino al numero di regole specificato. Ad esempio, se la complessità della password è impostata su 4, è necessario seguire le regole 1, 2, 3 e 4. Se la complessità della password è impostata su 2, è necessario seguire le regole 1 e 2. XClarity Administrator supporta le seguenti regole di complessità della password. • (1) Deve contenere almeno un carattere alfabetico e non deve avere più di due caratteri sequenziali, tra cui sequenze di caratteri alfabetici, cifre e tasti della tastiera QWERTY (ad esempio, "abc", "123" e "asd" non sono consentiti). • (2) Deve contenere almeno un numero (0-9). • (3) Deve contenere almeno *due* dei caratteri che seguono. – Caratteri alfabetici maiuscoli (A - Z) – Caratteri alfabetici minuscoli (a - z) – Caratteri speciali ; @ _ ! ' $ & + • (4) Non deve essere una ripetizione né l'inversione del nome utente. • (5) Non deve contenere consecutivamente più di due degli stessi caratteri (ad esempio, "aaa", "111" e "..." non sono ammessi). Se il valore è impostate su **0**, le password non sono necessarie per conformarsi alle regole di complessità.	**0 – 5**	**4**
Numero massimo di sessioni attive per un utente specifico	Numero massimo di sessioni attive per un utente specifico consentito in un determinato momento. Se il valore è impostato su **0**, il numero di sessioni attive consentito per un utente specifico è illimitato.	**1 – 20**	**3**
Forza utente a modificare la password al primo accesso	Indica se un utente deve modificare la password quando esegue per la prima volta il login a XClarity Administrator.	**Sì** o **No**	**Sì**

Passo 4. Fare clic su **Applica**.

Al termine

Una volta correttamente salvate, le nuove impostazioni vengono rese immediatamente effettive. La modifica dell'impostazione per il timeout sessione di inattività Web incide anche sulle sessioni attive.

I criteri di modifica delle password vengono applicati al successivo login o alla successiva modifica della password da parte dell'utente.

Configurazione delle impostazioni di crittografia sul server di gestione

È possibile configurare la versione SSL/TLS e le impostazioni di crittografia per il server di gestione.

Prima di iniziare

Prima di modificare le impostazioni nel server di gestione, verificare le considerazioni sulla crittografia (vedere Gestione della crittografia nella documentazione online di XClarity Administrator).

Informazioni su questa attività

La *modalità crittografica* determina la modalità di gestione delle comunicazioni sicure tra XClarity Administrator e tutti i sistemi gestiti. Se vengono implementate comunicazioni sicure, imposta le lunghezze delle chiavi di crittografia da utilizzare.

Nota: Indipendentemente dalla modalità crittografica selezionata, i generatori di bit casuali digitali approvati NIST vengono utilizzati sempre e per la crittografia simmetrica vengono usate solo chiavi a 128 bit o più lunghe.

Per modificare l'impostazione di sicurezza per i dispositivi gestiti, vedere Configurazione delle impostazioni di sicurezza per un server gestito.

Procedura

Per modificare le impostazioni di crittografia, completare le seguenti operazioni sul server di gestione.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza**.

Passo 2. Scegliere una delle seguenti modalità crittografiche da utilizzare per le comunicazioni sicure:

- **Compatibilità**. Questo è la modalità predefinita. È compatibile con le versioni firmware precedenti, i browser e gli altri client di rete che non implementano i rigorosi standard di sicurezza richiesti per la conformità NIST SP 800-131A.
- **NIST SP 800-131A**. Questa modalità è progettata per rispettare lo standard di conformità NIST SP 800-131A. XClarity Administrator è progettato per utilizzare sempre la crittografia interna e le connessioni di rete con crittografia sicura, dove disponibile. Tuttavia, in questa modalità, le connessioni di rete che utilizzano la crittografia non approvata da NIST SP 800-131A non sono autorizzate; ad esempio, i certificati TLS (Transport Layer Security) con firma SHA-1 o hash più debole verranno respinti.

  Se si seleziona questa modalità:

  – Per tutte le porte diverse dalla porta 8443, tutte le cifrature CBC TLS e quelle che non supportano Perfect Forward Secrecy sono disabilitate.

  – Le notifiche eventi potrebbero non essere inviate correttamente ad alcune sottoscrizioni di dispositivi mobili (vedere Inoltro di eventi a dispositivi mobili). Servizi esterni, come Android e iOS, presentano certificati firmati con SHA-1. Questo algoritmo non è conforme ai requisiti

più rigorosi della modalità NIST SP 800-131A. Pertanto, tutte le connessioni a questi servizi potrebbero non riuscire con un'eccezione del certificato o un errore di handshake.

Per ulteriori informazioni sulla NIST SP 800-131A conformità, vedere Implementazione della conformità NIST SP 800-131A.

Passo 3. Scegliere la versione minima del protocollo TLS da utilizzare per le connessioni client ad altri server (ad esempio il server LDAP). È possibile scegliere la seguente opzione

- **TLS1.2**. Applica i protocolli di crittografia TLS v1.2.
- **TLS1.3**. Applica i protocolli di crittografia TLS v1.3.

Passo 4. Scegliere la versione minima del protocollo TLS da utilizzare per le connessioni server (ad esempio il server Web). È possibile scegliere la seguente opzione.

- **TLS1.2**. Applica i protocolli di crittografia TLS v1.2.
- **TLS1.3**. Applica i protocolli di crittografia TLS v1.3.

Passo 5. Scegliere la versione minima del protocollo TLS da utilizzare per la distribuzione del sistema operativo XClarity Administrator e gli aggiornamenti dei driver di dispositivo del sistema operativo. È possibile scegliere la seguente opzione.

- **TLS1.2**. Applica i protocolli di crittografia TLS v1.2.
- **TLS1.3**. Applica i protocolli di crittografia TLS v1.3.

Nota: Solo i sistemi operativi con un processo di installazione che supporta l'algoritmo di crittografia selezionato o sicuro possono essere distribuiti e aggiornati tramite XClarity Administrator.

Passo 6. Selezionare la lunghezza della chiave crittografica e l'algoritmo hash da utilizzare per tutte le parti del certificato, inclusi il certificato CA radice, il certificato server e la CSR per i certificati con firma esterna.

- **RSA 2048-bit/SHA-256** (predefinito)

  Questa modalità può essere utilizzata quando i dispositivi gestiti sono in modalità di compatibilità, NIST SP 800-131A o sicurezza standard. Questa modalità *non può* essere utilizzata quando uno o più dispositivi gestiti sono in modalità **Sicurezza aziendale rigorosa**.

- **RSA 3072-bit/SHA-384**

  Questa modalità è richiesta quando i dispositivi gestiti sono in modalità **Sicurezza aziendale rigorosa**.

  Importante: Solo i server con XCC2 supportano le firme del certificato RSA-3072/SHA-384. Una volta configurato XClarity Administrator con un certificato basato su RSA-3072/SHA-384, la gestione dei dispositivi non XCC2 viene annullata. Per gestire i dispositivi non XCC2, è necessaria un'istanza XClarity Administrator separata.

Passo 7. Fare clic su **Applica**.

Passo 8. Riavviare XClarity Administrator (vedere Riavvio di XClarity Administrator).

Passo 9. Se è stata modificata la lunghezza della chiave crittografica, rigenerare il certificato radice dell'autorità di certificazione utilizzando la lunghezza della chiave e l'algoritmo hash corretti (vedere Rigenerazione o ripristino del certificato autofirmato del server di Lenovo XClarity Administrator o Distribuzione di certificati server personalizzati in Lenovo XClarity Administrator).

Al termine

Se si riceve un avviso per cui il certificato server non è attendibile per un dispositivo gestito, vedere Risoluzione di un certificato server non attendibile.

Configurazione delle impostazioni di sicurezza per un server gestito

È possibile configurare la versione SSL/TLS e le impostazioni di crittografia per i server gestiti.

Informazioni su questa attività

Considerare le seguenti implicazioni che comporta la modifica della modalità crittografica.

- La modifica dalla modalità **Sicurezza della compatibilità** o **Sicurezza standard** a **Sicurezza aziendale rigorosa** non è supportata.
- Se si esegue l'aggiornamento dalla modalità **Sicurezza della compatibilità** alla modalità **Sicurezza standard**, se i certificati importati o le chiavi pubbliche SSH non sono conformi, verrà visualizzato un avviso ma sarà comunque possibile aggiornare alla modalità **Sicurezza standard**.
- Se si esegue il downgrade dalla modalità **Sicurezza aziendale rigorosa** alla modalità **Sicurezza della compatibilità** o **Sicurezza standard**:
  - Il server viene automaticamente riavviato affinché la modalità di sicurezza sia resa effettiva.
  - Se la chiave FoD in modalità rigorosa manca o è scaduta su XCC2 e XCC2 utilizza un certificato TLS autofirmato, XCC2 rigenera il certificato TLS autofirmato basato sull'algoritmo conforme alla modalità Rigorosa standard. XClarity Administrator mostra un errore di connessione a causa di un errore del certificato. Per risolvere l'errore di certificato non attendibile, vedere Risoluzione di un certificato server non attendibile nella documentazione online di XClarity Administrator. Se XCC2 utilizza un certificato TLS personalizzato, XCC2 consente il downgrade e avverte l'utente della necessità di importare un certificato server basato sulla crittografia della modalità **Sicurezza standard**.
- La modalità **NIST SP 800-131A** non è supportata per i server con XCC2.
- Se la modalità crittografica di XClarity Administrator è impostata su TLS v1.2 e su un server gestito che utilizza l'autenticazione gestita è impostata una modalità di sicurezza su TLS v1.2, modificando la modalità di sicurezza del server su TLS v1.3 mediante XClarity Administrator o XCC, il server risulterà definitivamente offline.
- Se la modalità crittografica di XClarity Administrator è impostata su TLS v1.2 e si tenta di gestire un server con XCC e la modalità di sicurezza impostata su TLS v1.3, non è possibile gestire il server mediante l'autenticazione gestita.

È possibile modificare i valori delle impostazioni di sicurezza per i seguenti dispositivi.
- Server Lenovo ThinkSystem con processori Intel o AMD (ad eccezione di SR635/SR655)
- Server Lenovo ThinkSystem V2
- Server Lenovo ThinkSystem V3 con processori Intel o AMD
- Server Lenovo ThinkEdge SE350/SE450
- Server Lenovo System x

Procedura

Per modificare le impostazioni di sicurezza per server gestiti specifici, completare le seguenti operazioni.

Passo 1. Dal menu XClarity Administrator, fare clic su **Hardware → Server**. Verrà visualizzata la pagina Server contenente una vista tabulare di tutti i server gestiti.

Passo 2. Selezionare uno o più server.

Passo 3. Configurare la modalità di sicurezza.

1. Fare clic su **Tutte le azioni → Sicurezza → Imposta modalità di sicurezza del sistema** per visualizzare la finestra di dialogo Imposta modalità di sicurezza del sistema.

   Nella finestra di dialogo viene riportato il numero di server che è possibile configurare per ciascuna modalità. Passare il cursore su ogni numero per visualizzare un elenco di nomi di server applicabili.

2. Selezionare la modalità di sicurezza. É possibile selezionare uno dei seguenti valori.

   - **Sicurezza della compatibilità**. Selezionare questa modalità quando i servizi e i client richiedono crittografia non conforme a CNSA/FIPS. Questa modalità supporta un'ampia gamma di algoritmi di crittografia e consente l'abilitazione di tutti i servizi.
   - **NIST SP 800-131A**. Selezionare questa modalità per garantire la compatibilità con lo standard NIST SP 800-131A. Ciò include la restrizione delle chiavi RSA a 2048 bit o superiori, la restrizione degli hash utilizzati per le firme digitali a SHA-256 o più e la garanzia che vengano utilizzati solo gli algoritmi di crittografia simmetrica approvati NIST. Questa modalità richiede l'impostazione della modalità SSL/TLS sul **client del server TLS 1.2**.

     Questa modalità *non è* supportata per i server con XCC2.
   - **Sicurezza standard**. Questa è la modalità di sicurezza predefinita per server con XCC2 (solo server con XCC2). Selezionare questa modalità per garantire la compatibilità con lo standard FIPS 140-3. Per il funzionamento di XCC in modalità convalidata FIPS 140-3, è possibile abilitare solo i servizi che supportano la crittografia di livello FIPS 140-3. I servizi che non supportano la crittografia di livello FIPS 140-2/140-3 sono disabilitati per impostazione predefinita, ma possono essere abilitati, se necessario. Se è abilitato un servizio che utilizza la crittografia non di livello FIPS 140-3, XCC non può funzionare in modalità convalidata FIPS 140-3. Questa modalità richiede certificati di livello FIP.
   - **Sicurezza aziendale rigorosa**. Questa è la modalità più sicura (solo server con XCC2). Selezionare questa modalità per garantire la compatibilità con lo standard CNSA. Sono consentiti solo i servizi che supportano la crittografia di livello CNSA. I servizi non sicuri sono disabilitati per impostazione predefinita e non possono essere abilitati. Questa modalità richiede certificati di livello CNSA.

     XClarity Administrator utilizza le firme del certificato RSA-3072/SHA-384 per i server in modalità **Sicurezza aziendale rigorosa**.

     Importante:

     – Per utilizzare questa modalità, è necessario installare la chiave Feature On Demand di XCC2 per ogni elemento server con XCC2 selezionato.

     – In questa modalità, se XClarity Administrator utilizza un certificato autofirmato, XClarity Administrator deve utilizzare il certificato radice e il certificato server basati su RSA3072/SHA384. Se XClarity Administrator utilizza un certificato firmato esterno, XClarity Administrator deve generare una CSR basata su RSA3072/SHA384 e contattare la CA esterna per firmare un nuovo certificato server basato su RSA3072/SHA384.

     – Quando XClarity Administrator utilizza un certificato basato su RSA3072/SHA384, XClarity Administrator potrebbe scollegare i dispositivi diversi da: chassis e server Flex System (CMM), server ThinkSystem, server ThinkServer, server System x M4 e M5, switch Lenovo ThinkSystem serie DB, Lenovo RackSwitch, switch Flex System, switch Mellanox, dispositivi di storage ThinkSystem DE/DM, storage della libreria a nastro IBM e server ThinkSystem SR635/SR655 con firmware precedente alla versione 22C. Per continuare a gestire i dispositivi disconnessi, configurare un'altra istanza di XClarity Administrator con un certificato basato su RSA2048/SHA384.

3. Fare clic su **Applica**.

Passo 4. Configurare la versione minima del TLS.

1. Fare clic su **Tutte le azioni → Sicurezza → Imposta versione TLS del sistema** per visualizzare la finestra di dialogo Imposta versione TLS del sistema.
2. Selezionare la versione minima del protocollo TLS da utilizzare per le connessioni client ad altri server (ad esempio dal client LDAP a un server LDAP). Il valore viene configurato sui dispositivi selezionati che supportano questa impostazione. È possibile scegliere la seguente opzione.

- **TLS1.2**. Applica i protocolli di crittografia TLS v1.2.
- **TLS1.3**. Applica i protocolli di crittografia TLS v1.3.

Nota: I dispositivi System x e CMM supportano solo TLS v1.2.

3. Fare clic su **Applica**.

Utilizzo dei certificati di sicurezza

Lenovo XClarity Administrator utilizza i certificati SSL per stabilire le comunicazioni sicure e attendibile tra XClarity Administrator e i relativi dispositivi gestiti (come lo chassis e i processori di servizio dei server System x), nonché le comunicazioni con XClarity Administrator da parte degli utenti o con servizi differenti. Per impostazione predefinita, XClarity Administrator, i moduli CMM e i controller di gestione della scheda di base utilizzano i certificati generati da XClarity Administrator, autofirmati e pubblicati da un'autorità di certificazione interna.

Prima di iniziare

Questa sezione è dedicata agli amministratori con nozioni di base sugli standard SSL e sui certificati SSL, che ne conoscono la definizione e sanno come gestirli. Per informazioni generali sui certificati di chiave pubblica, vedere Pagina Web di X.509 su Wikipedia e Pagina Web - Profilo certificato di infrastruttura con chiave pubblica Internet X.509 e CRL (Certificate Revocation List) (RFC5280).

Informazioni su questa attività

Il certificato server autofirmato predefinito, generato in modo univoco in ogni istanza di XClarity Administrator, fornisce misure di sicurezza sufficienti per molti ambienti. È possibile delegare la gestione dei certificati a XClarity Administrator oppure avere un ruolo più attivo e personalizzare o sostituire i certificati server. XClarity Administrator fornisce le opzioni per personalizzare i certificati dell'ambiente. Ad esempio, è possibile scegliere di:

- Generare una nuova coppia di chiavi rigenerando l'autorità di certificazione interna e/o il certificato server finale che utilizzano i valori specifici dell'organizzazione.
- Generare una richiesta di firma del certificato che può essere inviata all'autorità di certificazione preferita per firmare un certificato personalizzato che può quindi essere caricato in XClarity Administrator ed essere utilizzato come certificato end-server per tutti i rispettivi servizi in hosting
- Scaricare il certificato del server nel sistema locale in modo da importarlo nell'elenco del browser Web dei certificati attendibili.

XClarity Administrator fornisce diversi servizi che accettano le connessioni SSL/TLS in entrata. Quando un client, come un dispositivo gestito o un browser web, si collega a uno di questi servizi, XClarity Administrator fornisce il rispettivo *certificato server* per essere identificato dal client che sta tentando di connettersi. Il client deve mantenere un elenco di certificati ritenuti attendibili. Se il certificato server di XClarity Administrator non è nell'elenco, il client si disconnette da XClarity Administrator per evitare lo scambio di informazioni di sicurezza riservate con un'origine non attendibile.

XClarity Administrator funge da client durante la comunicazione con dispositivi gestiti e servizi esterni. Quando XClarity Administrator si connette a un dispositivo o a un servizio esterno, il dispositivo o il servizio esterno fornisce il rispettivo certificato server per essere identificato da XClarity Administrator. XClarity Administrator gestisce un elenco di certificati ritenuti attendibili. Se il *certificato attendibile* fornito dal dispositivo gestito o dal servizio esterni non è nell'elenco, XClarity Administrator si disconnette dal dispositivo gestito o dal servizio esterno al fine di evitare lo scambio di eventuali informazioni di sicurezza riservate con un'origine non attendibile.

La seguente categoria di certificati viene utilizzata dai servizi di XClarity Administrator e deve essere considerata attendibile da qualsiasi client che vi si connette.

- **Certificato server**. Durante l'avvio iniziale vengono generati una chiave univoca e un certificato autofirmato. Entrambi vengono utilizzati come autorità di certificazione radice predefinita, gestibile dalla pagina Autorità di certificazione tra le impostazioni di sicurezza di XClarity Administrator. Non è necessario rigenerare questo certificato radice, a meno che la chiave non sia stata compromessa o la politica della propria organizzazione non preveda la sostituzione periodica di tutti i certificati (vedere Rigenerazione o ripristino del certificato autofirmato del server di Lenovo XClarity Administrator).

  Durante la configurazione iniziale viene generata una chiave separata, viene creato un certificato server e firmato un certificato dall'autorità di certificazione interna. Questo certificato viene utilizzato come certificato server predefinito di XClarity Administrator. Esso si rigenera automaticamente ogni volta che XClarity Administrator rileva che i rispettivi indirizzi di rete (indirizzi DNS o IP) sono stati modificati per garantire che il certificato contenga gli indirizzi corretti per il server. Può essere personalizzato e generato su richiesta (vedere Rigenerazione o ripristino del certificato autofirmato del server di Lenovo XClarity Administrator).

  È possibile scegliere di utilizzare un certificato del server con firma esterna invece del certificato server autofirmato predefinito, generando una richiesta di firma del certificato (CSR), una CSR firmata da un'autorità di certificazione radice privata o commerciale e importando quindi la catena di certificati completa in XClarity Administrator (vedere Distribuzione di certificati server personalizzati in Lenovo XClarity Administrator).

  Se si sceglie di utilizzare il certificato del server autofirmato predefinito, è consigliabile importare il certificato del server nel browser Web come autorità radice attendibile per evitare messaggi di errore del certificato nel browser (vedere Importazione del certificato dell'Autorità di certificazione in un browser Web).
- **Certificato di distribuzione del sistema operativo**. Un certificato separato viene utilizzato dal servizio di distribuzione del sistema operativo per garantire che il programma di installazione del sistema operativo possa connettersi in modo sicuro al servizio di distribuzione durante il processo di installazione del sistema operativo. Se la chiave è stata compromessa, è possibile rigenerarla riavviando il server di gestione.

La seguente categoria (archivi attendibili) di certificati viene utilizzata dai client di XClarity Administrator.

- **Certificati attendibili**.

  Questo archivio attendibile gestisce i certificati utilizzati per stabilire una connessione sicura alle risorse locali quando XClarity Administrator viene utilizzato come client. Esempi di risorse locali sono i dispositivi gestiti, il software locale per l'inoltro di eventi e un server LDAP esterno.
- **Certificati servizi esterni**. Questo archivio attendibile gestisce i certificati utilizzati per stabilire una connessione sicura con servizi esterni quando XClarity Administrator viene utilizzato come client. Esempi di servizi esterni sono i servizi online del supporto Lenovo utilizzati per recuperare le informazioni sulla garanzia o creare ticket di assistenza, il software esterno (come Splunk) a cui possono essere inoltrati gli eventi e i server delle notifiche push Apple e Google, se le notifiche push sono abilitate per un dispositivo iOS o Android di Lenovo XClarity Mobile. Contiene certificati attendibili preconfigurati, provenienti da autorità di certificazione radice di determinati fornitori da autorità di certificazione comunemente attendibili e note in tutto il mondo (come Digicert e Globalsign).

  Quando si configura XClarity Administrator per utilizzare una funzione che richiede una connessione a un altro servizio esterno, fare riferimento alla documentazione per determinare se è necessario aggiungere manualmente un certificato a questo archivio attendibile.

  Nota: i certificati in questo archivio attendibile non sono attendibili quando si stabiliscono connessioni per altri servizi (come LDAP) a meno che anche questi non vengano aggiunti all'archivio attendibile principale dei certificati attendibili. La rimozione di certificati da questo archivio attendibile impedisce il corretto funzionamento di questi servizi.

XClarity Administrator supporta firme del certificato RSA-3072/SHA-384, RSA-2048/SHA-256 e ECDSA p256/SHA-256. A seconda della configurazione, potrebbero essere supportati altri algoritmi come uno SHA-1 di livello superiore o hash SHA. Tenere in considerazione la modalità crittografica selezionata in XClarity Administrator (vedere Configurazione delle impostazioni di crittografia sul server di gestione), le impostazioni di sicurezza selezionate per i server gestiti (Configurazione delle impostazioni di sicurezza per un server gestito) e le funzionalità di altri software e dispositivi nel proprio ambiente. I certificati ECDSA basati su alcune curve ellittiche (come p256) sono supportati nella pagina Certificati attendibili e nella catena di firme del certificato di XClarity Administrator ma attualmente *non* possono essere utilizzati dal certificato server di XClarity Administrator.

Nota: XClarity Administrator utilizza le firme del certificato RSA- 3072/SHA-384 per server con XCC2 in modalità Rigorosa.

Installazione di un certificato del server con firma esterna personalizzato

È possibile scegliere di utilizzare un certificato server firmato da un'autorità di certificazione (CA) privata o commerciale.

Prima di iniziare

Verificare che l'Autorità di certificazione radice sia quella generata dall'organizzazione e utilizzata per firmare i certificati all'interno di tale organizzazione o che sia un'autorità di certificazione comunemente attendibile e note in tutto il mondo (vedere Pagina Web - Elenco autorità di certificazione attendibili).

Accertarsi che gli algoritmi per le chiavi e le firme del certificato CA radice siano supportati. Sono supportate solo le firme RSA-3072/SHA-384 e RSA-2048/SHA-256. Al momento, le firme RSA-PSS non sono supportate.

Verificare che in tutti i dispositivi gestiti sia installato il firmware più recente prima di iniziare attività che potrebbero influire sulle connessioni tra i dispositivi gestiti. Per aggiornare il firmware sui dispositivi gestiti, vedere Aggiornamento del firmware sui dispositivi gestiti.

Verificare che XClarity Administrator comunichi correttamente tutti i dispositivi gestiti, facendo clic su **Hardware** poi sul tipo di dispositivo (chassis o server). Verrà visualizzata una pagina contenente una vista tabulare di tutti i dispositivi gestiti di tale tipo. In caso vi siano dispositivi con stato "Offline", verificare che la connettività di rete sia attiva tra il server di gestione e il dispositivo e risolvere certificati server non attendibili, se necessario (vedere Risoluzione di un certificato server non attendibile).

Informazioni su questa attività

Quando si installa un certificato del server con firma esterna personalizzato in XClarity Administrator oppure un controller di gestione della scheda di base o CMM, è necessario fornire il bundle di certificati che contiene l'intera catena di firma della CA.

Quando si installa un certificato server personalizzato in uno chassis o in un server non gestito da XClarity Administrator, installare il bundle di certificati in CMM prima di installarlo in tutti i controller di gestione in CMM.

Quando si installa un certificato server personalizzato in uno chassis gestito, è innanzitutto necessario aggiungere la catena di firma della CA all'archivio attendibile di XClarity Administrator, installare il certificato server in ogni controller di gestione e CMM, quindi caricare il certificato server su XClarity Administrator. Nota: questa operazione può essere facilmente ignorata considerando attendibili/aggiungendo tutti i certificati CA radice, ma non ciascuna catena di certificati da ogni dispositivo gestito. Il numero di certificati importati deve essere uguale al numero di certificati CA radice (certificati CA radice + tutti i certificati CA

intermedi). Per ulteriori informazioni, vedere Distribuzione di certificati server personalizzati in dispositivi gestiti.

È necessario aggiungere il certificato radice CA e tutti i certificati intermedi, uno alla volta, all'archivio attendibile di XClarity Administrator. L'ordine è indifferente. Ogni certificato deve essere installato una volta, pertanto se tutti i dispositivi utilizzano la stessa CA e gli stessi certificati intermedi, è sufficiente che la CA e ogni certificato intermedio siano installati nell'archivio attendibile di XClarity Administrator una sola volta. Se si utilizza più di una CA o una CA intermedia, assicurarsi che ogni certificato radice CA univoco o certificato intermedio utilizzato nella catena di firma di un dispositivo gestito venga importato attenendosi alla procedura descritta di seguito.

Suggerimento: se il nuovo certificato server non è stato firmato da una terza parte attendibile, alla successiva connessione a XClarity Administrator nel browser verrà visualizzato un messaggio di sicurezza e una finestra di dialogo in cui verrà richiesto di accettare il nuovo certificato nel browser. Per evitare i messaggi di sicurezza, è possibile importare un certificato server scaricato nell'elenco dei certificati attendibili del browser Web. Per ulteriori informazioni sull'importazione dei certificati server, vedere Importazione del certificato dell'Autorità di certificazione in un browser Web.

Distribuzione di certificati server personalizzati in Lenovo XClarity Administrator

È possibile scegliere di generare una richiesta di firma del certificato (Certificate Signing Request, CSR) da far firmare all'autorità di certificazione della propria organizzazione o a un'autorità di certificazione di terze parti. La richiesta di firma del certificato crea una catena di certificati completa che è possibile importare e utilizzare al posto dei singoli certificati predefiniti firmati internamente.

Prima di iniziare

Verificare che i dettagli del certificato includano i seguenti requisiti.

- Utilizzo chiavi deve contenere
  - Accordo chiave
  - Firma digitale
  - Crittografia a chiave
- Utilizzo chiavi avanzato deve contenere
  - Server di autenticazione (1.3.6.1.5.5.7.3.1)
  - Autenticazione client (1.3.6.1.5.5.7.3.2)

Informazioni su questa attività

Attenzione: Se NIST SP 800-131A è abilitato (vedere Implementazione della conformità NIST SP 800-131A) e si utilizza o si intende utilizzare certificati personalizzati o con firma esterna in un ambiente NIST, tutti i certificati nella catena devono essere basati sulle funzioni di hash SHA-256.

Una volta caricato il certificato server, XClarity Administrator tenta di eseguire il provisioning del nuovo certificato CA su tutti i dispositivi gestiti. Se il processo di provisioning riesce, XClarity Administrator inizia subito a utilizzare il nuovo certificato server. Se il processo non riesce, vengono visualizzati messaggi di errore nei quali viene specificato di risolvere i problemi manualmente prima di applicare il certificato server appena importato. Dopo aver corretto gli errori, completare l'installazione del certificato caricato in precedenza.

Nota: Se XClarity Administrator già utilizzava un certificato firmato dalla stessa autorità radice, la CA non deve essere inviata ai dispositivi e XClarity Administrator inizia subito a utilizzare il certificato.

Dopo aver caricato un certificato in XClarity Administrator v1.1.0 e versioni precedenti, il server Web riavvia e termina automaticamente tutte le sessioni del browser. XClarity Administrator v1.1.1 e versioni successive

inizia a utilizzare il nuovo certificato senza terminare le sessioni esistenti. Tutte le nuove sessioni vengono stabilite utilizzando il nuovo il certificato. Per vedere il nuovo certificato in uso, riavviare il browser Web.

Procedura

Per generare e distribuire un certificato del server con firma esterna personalizzato in Lenovo XClarity Administrator, attenersi alla procedura descritta di seguito.

Passo 1. Creare e scaricare una richiesta di firma del certificato (CSR) per XClarity Administrator.

a. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Sicurezza** per visualizzare la pagina Sicurezza

b. Fare clic su **Certificato server** nella sezione Gestione certificati per visualizzare la pagina Certificato server.

c. Fare clic sulla scheda **Genera CSR (Certificate Signing Request)**.

d. Compilare i campi per la richiesta.
- Paese o regione
- Stato o provincia
- Città o località
- Organizzazione
- Unità organizzativa (opzionale)
- Nome comune

Attenzione: Selezionare un nome comune corrispondente all'indirizzo IP o al nome host utilizzato da XClarity Administrator per connettersi al dispositivo gestito. La mancata selezione del valore corretto può comportare la presenza di connessioni non attendibili.

e. Personalizzare i nomi alternativi dell'oggetto (SAN) che vengono aggiunti all'estensione X.509 "subjectAltName" quando viene generata una richiesta CSR.

Per impostazione predefinita, XClarity Administrator definisce automaticamente i nomi alternativi dell'oggetto (SAN) per la richiesta CSR in base all'indirizzo IP e al nome host rilevati dalle interfacce di rete del sistema operativo guest di XClarity Administrator. È possibile personalizzare, eliminare o aggiungere questi valori SAN.

Il nome specificato deve essere valido per il tipo selezionato:
- **directoryName** (ad esempio, `cn=lxca-example,ou=dcg,dc=company,dc=com`)
- **dNSName** (ad esempio, `lxca-example.dcg.company.com`)
- **ipAddress** (ad esempio, `192.0.2.0`)
- **registeredID** (ad esempio, `1.2.3.4.55.6.5.99`)
- **rfc822Name** (ad esempio, `example@company.com`)
- **uniformResourceIdentifier** (ad esempio, `https://lxca-dev.dcg.company.com/example`)

Nota: Tutte le reti SAN elencate nella tabella vengono convalidate, salvate e aggiunte alla richiesta CSR solo dopo che l'utente ha generato la richiesta CSR nel passaggio successivo.

f. Fare clic su **Genera file CSR**. Il certificato server viene visualizzato nella finestra di dialogo Richiesta di firma del certificato.

g. Fare clic su **Salva su file** per salvare il certificato server nel server host.

Passo 2. Fornire la CSR a un'autorità di certificazione (CA) attendibile. L'autorità di certificazione firma la CSR e risponde con un certificato server.

Passo 3. Caricare il certificato del server con firma esterna su XClarity Administrator. Il contenuto del certificato deve essere un bundle contenente il certificato radice dell'autorità di certificazione, i certificati intermedi e il certificato server.

a. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Sicurezza** per visualizzare la pagina Sicurezza.
b. Fare clic su **Certificato server** nella sezione Gestione certificati.
c. Fare clic sulla scheda **Carica certificato**.
d. Fare clic su **Carica certificato** per visualizzare la finestra di dialogo Carica certificato.
e. Specificare un file bundle di certificati in formato PEM, DER o PKCS7 oppure incollare il bundle di certificati in formato PEM.
f. Fare clic su **Carica** per caricare il certificato server e archiviare il certificato nell'archivio attendibile di XClarity Administrator.

Distribuzione di certificati server personalizzati in dispositivi gestiti

È possibile distribuire certificati server personalizzati in dispositivi gestiti caricando e installando il bundle di certificati con firma esterna mediante CMM e il controller di gestione per tali dispositivi.

Prima di iniziare

Verificare che il firmware più recente sia installato in tutti i dispositivi gestiti (vedere Aggiornamento del firmware sui dispositivi gestiti).

Quando si genera una richiesta di firma del certificato (CSR) per i certificati personalizzati, assicurarsi di selezionare un nome comune che corrisponda all'indirizzo IP o al nome host utilizzato per identificare il dispositivo. La mancata selezione del valore corretto può comportare la presenza di connessioni non attendibili.

Assicurarsi di ottenere un bundle di certificati che contenga l'intera catena di firma, dal certificato server finale al certificato radice (base) della CA attendibile, che è possibile utilizzare per verificare l'intera catena di certificati attendibili.

Non modificare il certificato server di Lenovo XClarity Administrator mentre un dispositivo gestito è "Offline". È importante ripristinare la connessione prima di modificare Lenovo XClarity Administrator poiché, in caso contrario, potrebbe essere necessario intervenire ulteriormente per risolvere i problemi di connettività (vedere Risoluzione di un certificato server non attendibile).

Informazioni su questa attività

In questa sezione vengono forniti consigli utili a garantire una comunicazione sempre ottimale tra Lenovo XClarity Administrator e i dispositivi gestiti. Per istruzioni dettagliate su come generare una CSR e importare un certificato firmato, vedere la documentazione del dispositivo utilizzato.

Se Lenovo XClarity Administrator gestisce uno o più chassis, server rack e server tower, e i certificati con firma interna predefiniti di Lenovo XClarity Administrator sono attualmente installati in Lenovo XClarity Administrator e nei dispositivi gestiti, è possibile distribuire un certificato server personalizzato.

Se il certificato del server con firma esterna viene installato nel dispositivo *prima* del tentativo di gestione del dispositivo da Lenovo XClarity Administrator, non sarà necessario eseguire ulteriori azioni. Per distribuire un certificato server personalizzato nei dispositivi gestiti tramite Lenovo XClarity Administrator, è necessario eseguire una delle seguenti procedure per garantire la connettività continua tra il server di gestione e i dispositivi gestiti.

Procedura

Per distribuire il certificato del server con firma esterna nei server o negli chassis gestiti, attenersi a una delle procedure descritte di seguito.

- Se Lenovo XClarity Administrator utilizza un certificato firmato dalla stessa autorità di certificazione dei dispositivi gestiti, attenersi alla procedura descritta in Distribuzione di certificati server personalizzati in Lenovo XClarity Administrator *prima* di installare i certificati nei dispositivi gestiti. L'installazione della catena di certificati di Lenovo XClarity Administrator provenienti dalla stessa CA assicura non solo che la catena di certificati si trova nell'archivio attendibile di Lenovo XClarity Administrator, ma anche che Lenovo XClarity Administrator è in grado di considerare attendibili i dispositivi dopo l'installazione dei certificati con firma esterna.
- Aggiungere i certificati con firma esterna nelle catene di firma CA all'archivio attendibile di Lenovo XClarity Administrator.

  È necessario aggiungere il certificato radice CA e tutti i certificati intermedi, uno alla volta, all'archivio attendibile di Lenovo XClarity Administrator. L'ordine è indifferente. Ogni certificato deve essere installato una volta, pertanto se tutti i dispositivi utilizzano la stessa CA e gli stessi certificati intermedi, è sufficiente che la CA e ogni certificato intermedio siano installati nell'archivio attendibile di Lenovo XClarity Administrator una sola volta. Se si utilizza più di una CA o una CA intermedia, assicurarsi che ogni certificato radice CA univoco o certificato intermedio utilizzato nella catena di firma di un dispositivo gestito venga importato attenendosi alla procedura descritta di seguito.

  Nota: Non aggiungere i certificati server non CA finali durante questa procedura.

  Attenersi alla procedura descritta di seguito per ogni certificato nel bundle.

  1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Sicurezza** per visualizzare la pagina Sicurezza.
  2. Fare clic su **Certificati attendibili** in Gestione certificati nel riquadro di navigazione a sinistra.
  3. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo Aggiungi certificato.
  4. Specificare un file del certificato in formato PEM o DER oppure incollare il certificato in formato PEM.
  5. Fare clic su **Crea** per creare il certificato.

  Una volta installata la catena di firma CA, Lenovo XClarity Administrator riterrà attendibili le connessioni ai server CIM su CMM e il controller di gestione in cui è installato il certificato del server con firma esterna.
- Importare i certificati con firma esterna nei dispositivi gestiti.

  Nota: Se i certificati necessari non sono presenti nell'archivio attendibile di Lenovo XClarity Administrator, la connettività tra Lenovo XClarity Administrator e il dispositivo gestito andrà persa. Attenersi alla procedura descritta in Risoluzione di un certificato server non attendibile per ripristinare la connessione.

  Importante: Questa opzione comporta una temporanea perdita della connettività, pertanto è consigliabile scegliere una delle procedure precedenti.

Rigenerazione o ripristino del certificato autofirmato del server di Lenovo XClarity Administrator

È possibile generare una nuova autorità di certificazione o un nuovo certificato server per sostituire i certificati autofirmati correnti o per reintegrare un certificato generato da Lenovo XClarity Administrator qualora XClarity Administrator utilizzi un certificato del server con firma esterna personalizzato. Il nuovo certificato autofirmato del server viene quindi utilizzato dai server di autenticazione, HTTPS e CIM in XClarity Administrator. sottoposto a provisioning automatico in tutti i dispositivi gestiti.

Prima di iniziare

Quando si rigenera o si carica il certificato XClarity Administrator, XClarity Administrator viene riavviato.

Se viene generato un nuovo certificato CA, questo verrà automaticamente distribuito nell'archivio attendibile di ogni CMM e controller di gestione della scheda di base in tutti gli chassis, i server rack e i server tower gestiti per mantenere le connessioni del server di autenticazione attendibili. Se si verifica un errore durante la distribuzione del certificato radice CA, scaricare il certificato dalla pagina dell'Autorità di certificazione e importarlo manualmente nell'archivio attendibile dei dispositivi gestiti in cui il provisioning non è stato eseguito correttamente, prima di generare un nuovo certificato server.

Se si intende rigenerare il certificato CA, trovare il tempo di rigenerare la CA, risolvere gli eventuali errori di provisioning e rigenerare il certificato server entro un breve periodo di tempo.

Dopo la generazione di un nuovo certificato radice CA, potrebbero verificarsi errori di comunicazione o potrebbe non essere possibile eseguire il login a un dispositivo finché il certificato server non sarà stato rigenerato e firmato.

Importante: Per XClarity Administrator v1.1.1 e versioni precedenti, è necessario importare il certificato radice CA nell'archivio attendibile di ogni CMM e controller di gestione. Per ulteriori informazioni sull'importazione del certificato radice CA, vedere la documentazione relativa a CMM e al controller di gestione

Procedura

Per ripristinare un certificato autofirmato del server su XClarity Administrator, attenersi alla procedura descritta di seguito.

Nota: Il certificato server attualmente in uso su XClarity Administrator, sia esso autofirmato o con firma esterna, rimarrà in uso finché non verrà rigenerato e firmato il nuovo certificato server.

Passo 1. **Facoltativo:** generare un nuovo certificato radice CA.

a. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Sicurezza** per visualizzare la pagina Sicurezza.

b. Fare clic su **Autorità di certificazione** nella sezione Gestione certificati.

c. Fare clic su **Rigenera certificato radice autorità di certificazione**.

Se il certificato e la chiave CA vengono rigenerati correttamente, verrà visualizzata una finestra di dialogo in cui viene mostrato lo stato dei processi per il provisioning di tale certificato come certificato attendibile LDAP in tutti i CMM e i controller di gestione (per i server Converged, NeXtScale e System x). Questa finestra di dialogo, come la pagina di monitoraggio dei processi, mostra l'esito positivo o negativo di ognuno di tali processi di provisioning.

Se uno dei processi di provisioning non riesce, attenersi alla procedura descritta di seguito per scaricare il certificato radice CA e importare manualmente il certificato radice come certificato LDAP attendibile in tutti i dispositivi per cui il processo non è riuscito.

Passo 2. **Facoltativo:** scaricare il certificato radice CA nel sistema host e importarlo nel browser Web.

a. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Sicurezza** per visualizzare la pagina Sicurezza.

b. Fare clic su **Autorità di certificazione** nella sezione Gestione certificati.

c. Fare clic su **Scarica certificato radice autorità di certificazione**. Il certificato radice CA corrente è visualizzato nella finestra di dialogo Certificato radice autorità di certificazione.

d. Fare clic su **Salva su file** per salvare il certificato radice CA nel sistema host.

e. Seguire le istruzioni per il browser Web utilizzato e il browser Web di altri utenti che eseguiranno l'accesso a XClarity Administrator per importare il certificato come autorità radice attendibile.

Passo 3. Rigenerare un nuovo certificato server e firmare il certificato con il nuovo certificato radice CA.

a. Dalla pagina Sicurezza fare clic su **Certificato server** nella sezione Gestione certificati.

b. Fare clic sulla scheda **Rigenera certificato server**.

c. Compilare i campi nella pagina Rigenera certificato server:
   - Paese o regione
   - Stato o provincia
   - Città o località
   - Organizzazione
   - Unità organizzativa
   - Nome comune
   - Data Non valido prima
   - Ora Non valido prima
   - Data Non valido dopo
   - Ora Non valido dopo

d. Fare clic su **Rigenera certificato**.

e. Se si rigenerano certificati server autofirmati su CMM e controller di gestione gestiti (per server Converged, NeXtScale, ThinkSystem, e System x), dopo aver rigenerato il certificato su ogni dispositivo, importare il nuovo certificato del dispositivo nell'archivio attendibile di XClarity Administrator (vedere Risoluzione di un certificato server non attendibile). In alternativa, è possibile scaricare manualmente il certificato dal dispositivo e importarlo in XClarity Administrator nella pagina Certificati attendibili.

In XClarity Administrator v1.1.0 e versioni precedenti, dopo la rigenerazione di un certificato il server Web si riavvia e termina automaticamente tutte le sessioni del browser. In XClarity Administrator v1.1.1 e versioni successive XClarity Administrator inizia a utilizzare il nuovo certificato senza terminare le sessioni esistenti. Le nuove sessioni verranno stabilite utilizzando il nuovo il certificato. Per vedere il nuovo certificato in uso, riavviare il browser Web.

Passo 4. Se si rigenerano certificati server autofirmati su CMM e controller di gestione gestiti (per server Converged, NeXtScale, ThinkSystem, e System x), dopo aver rigenerato il certificato su ogni dispositivo, importare il nuovo certificato del dispositivo nell'archivio attendibile di XClarity Administrator (vedere Risoluzione di un certificato server non attendibile). In alternativa, è possibile scaricare manualmente il certificato dal dispositivo e importarlo in XClarity Administrator nella pagina Certificati attendibili.

Risoluzione di un certificato server non attendibile

Il certificato server utilizzato per stabilire una connessione sicura a un dispositivo gestito può diventare non attendibile. Se il problema è dovuto a una versione di livello inferiore del certificato radice CA del dispositivo o del certificato autofirmato del dispositivo nell'archivio attendibile di Lenovo XClarity Administrator, XClarity Administrator è in grado di risolvere il certificato server non attendibile.

Informazioni su questa attività

Se un dispositivo gestito diventa non attendibile, XClarity Administrator impedisce la comunicazione con tale dispositivo, evitando di eseguire operazioni di inventario o di gestione su di esso.

Procedura

Per risolvere un certificato server non attendibile relativo a un dispositivo gestito, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Hardware**, quindi sul tipo di dispositivo (**Chassis**, **Server**, **Storage** o **Switch**). Verrà visualizzata una pagina contenente una vista tabulare di tutti i dispositivi gestiti di tale tipo.

Passo 2. Selezionare uno dispositivo specifico nello stato "Offline".

Passo 3. Fare clic su **Tutte le azioni → Sicurezza → Risolvi certificati non attendibili**.

Passo 4. Fare clic su **Installa certificato**.

XClarity Administrator recupera il certificato corrente dal dispositivo di destinazione. Se il certificato è differente dal certificato attendibile per il dispositivo nell'archivio attendibile XClarity Administrator, il nuovo certificato viene posizionato nell'archivio attendibile XClarity Administrator, sovrascrivendo il precedente certificato del dispositivo.

Se questo non risolve il problema, assicurarsi che la connettività di rete sia attiva tra XClarity Administrator e il dispositivo.

Download del certificato server

È possibile scaricare una copia del certificato server corrente, in formato PEM o DER, nel sistema locale. Quindi, è possibile importare il certificato nel browser Web o in altre applicazioni (come Lenovo XClarity Mobile o Lenovo XClarity Integrator).

Procedura

Per scaricare il certificato server, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Sicurezza** per visualizzare la pagina Sicurezza.

Passo 2. Fare clic su **Certificato server** nella sezione Gestione certificati. Verrà visualizzata la pagina Certificato server.

Passo 3. Fare clic sulla scheda **Scarica certificato**.

Passo 4. Fare clic su **Scarica certificato**.

Passo 5. Fare clic su **Salva come DER** o **Salva come PEM** per salvare il file del certificato server in formato DER o PEM nel sistema locale.

Importazione del certificato dell'Autorità di certificazione in un browser Web

Per evitare i messaggi di avvertenza di sicurezza del browser Web durante l'accesso a Lenovo XClarity Administrator, è possibile scaricare una copia del certificato dell'Autorità di certificazione (CA) corrente, in formato PEM o DER, nel sistema locale e importare tale certificato nell'elenco dei certificati attendibili del browser Web in uso.

Informazioni su questa attività

XClarity Administrator supporta firme del certificato RSA-3072/SHA-384, RSA-2048/SHA-256 e ECDSA p256/SHA-256. A seconda della configurazione, potrebbero essere supportati altri algoritmi come uno SHA-1 di livello superiore o hash SHA. Tenere in considerazione la modalità crittografica selezionata in XClarity Administrator (vedere Configurazione delle impostazioni di crittografia sul server di gestione), le impostazioni di sicurezza selezionate per i server gestiti (Configurazione delle impostazioni di sicurezza per un server gestito) e le funzionalità di altri software e dispositivi nel proprio ambiente. I certificati ECDSA basati su alcune curve ellittiche (come p256) sono supportati nella pagina Certificati attendibili e nella catena di firme del certificato di XClarity Administrator ma attualmente *non* possono essere utilizzati dal certificato server di XClarity Administrator.

Nota: XClarity Administrator utilizza le firme del certificato RSA- 3072/SHA-384 per server con XCC2 in modalità Rigorosa.

Procedura

Per scaricare il certificato server, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Sicurezza** per visualizzare la pagina Sicurezza.

Passo 2. Fare clic su **Autorità di certificazione** nella sezione Gestione certificati. Verrà visualizzata la pagina Autorità di certificazione.

Passo 3. Fare clic su **Scarica certificato radice autorità di certificazione**.

Passo 4. Fare clic su **Salva come DER** o **Salva come PEM** per salvare il file del certificato server in formato DER o PEM nel sistema locale.

Passo 5. Importare il certificato scaricato nell'elenco dei certificati radice attendibili dell'autorità per il browser in uso.

- **Firefox:**
  1. Aprire il browser e fare clic su **Strumenti → Opzioni → Avanzate**.
  2. Fare clic sulla scheda **Certificati**.
  3. Fare clic su **Mostra certificati**.
  4. Fare clic su **Importa** e accedere alla posizione in cui è stato scaricato il certificato.
  5. Selezionare il certificato e fare clic su **Apri**.
- **Internet Explorer:**
  1. Aprire il browser e fare clic su **Strumenti → Opzioni Internet → Contenuto**.
  2. Fare clic su **Certificati** per visualizzare un elenco di tutti i certificati attualmente attendibili.
  3. Fare clic su **Importa** per visualizzare la finestra Importazione guidata certificati.
  4. Completare l'importazione guidata del certificato.

Aggiunta e sostituzione di un elenco di revoche di certificati

Un *elenco di revoche di certificati* è un elenco di certificati revocati e non più attendibili. Un certificato può essere revocato se emesso in modo errato dalla CA o se la relativa chiave è stata compromessa, persa o rubata.

Procedura

Per aggiungere un nuovo elenco di revoche di certificati o per sostituire un elenco di revoche di certificati esistente, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Sicurezza** per visualizzare la pagina Sicurezza.

Passo 2. Fare clic su **Elenchi di revoche dei certificati** in Gestione certificati nel riquadro di navigazione a sinistra. Nella pagina Elenchi di revoche dei certificati è visualizzato un elenco di tutti gli elenchi di revoche di certificati.

Passo 3. Fare clic su **Aggiungi/Sostituisci CRL** per aggiungere un elenco di revoche di certificati oppure selezionare un elenco di revoche di certificati e fare clic su **Aggiungi/Sostituisci CRL** per sostituire il CRL.

Passo 4. Specificare il file dell'elenco di revoche di certificati, in formato PEM o DER, o incollare il certificato in formato PEM.

Passo 5. Fare clic su **Crea** per creare l'elenco di revoche di certificati.

Abilitazione incapsulamento

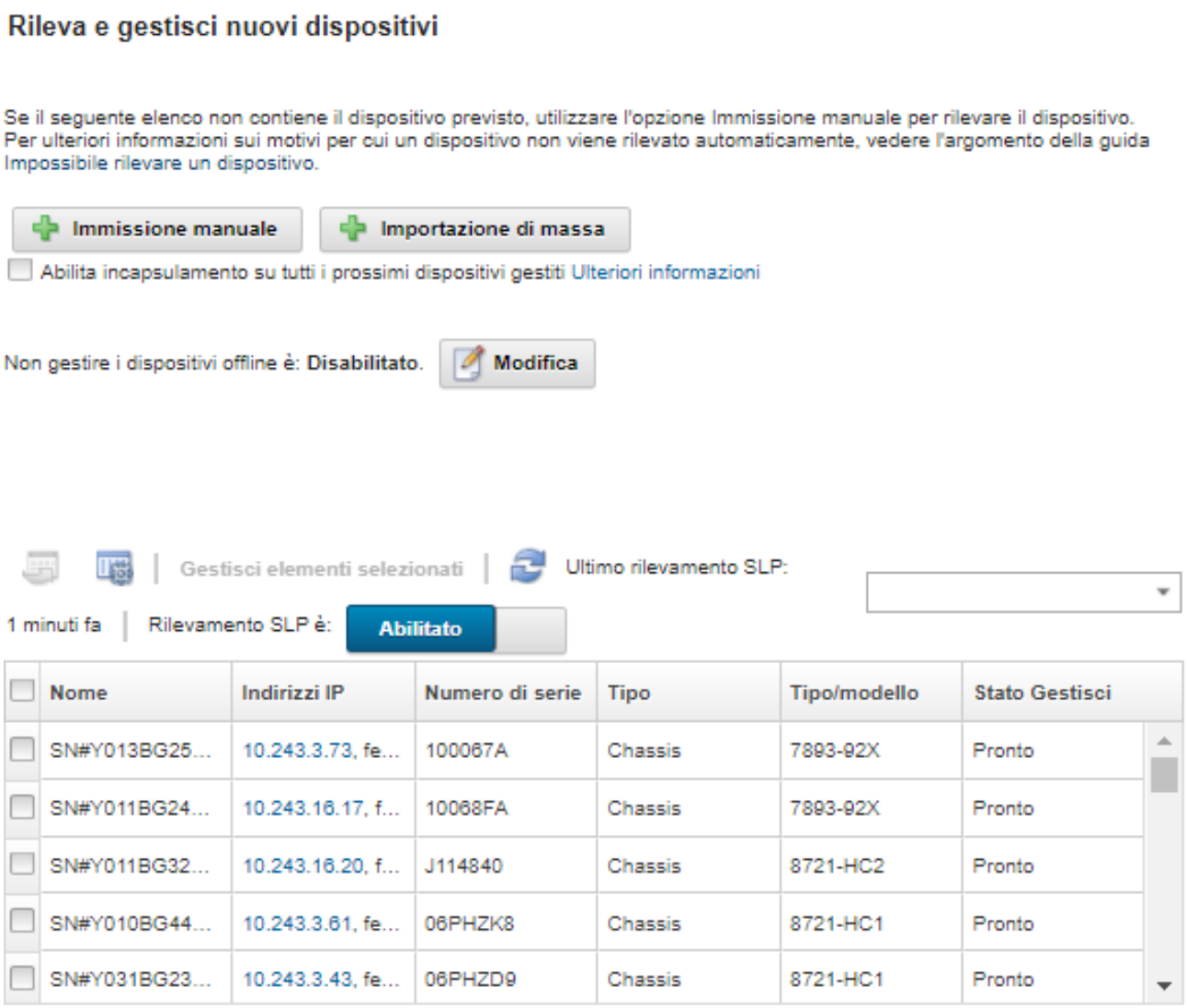
Quando si gestiscono gli chassis e i server Lenovo in Lenovo XClarity Administrator, è possibile configurare Lenovo XClarity Administrator affinché modifichi le regole del firewall per i dispositivi in modo che le richieste in entrata vengano accettate solo da Lenovo XClarity Administrator. Questo processo è detto

incapsulamento. É inoltre possibile abilitare o disabilitare l'incapsulamento su chassis e server già gestiti da Lenovo XClarity Administrator.

Quando abilitato sui dispositivi che supportano l'incapsulamento, Lenovo XClarity Administrator modifica la modalità di incapsulamento del dispositivo in "encapsulationLite" e le regole del firewall sul dispositivo per limitare le richieste in entrata solo a quelle provenienti da Lenovo XClarity Administrator.

Se disabilitata, la modalità di incapsulamento è impostata su "normale". Se l'incapsulamento è stato precedentemente abilitato sui dispositivi, le regole del firewall per l'incapsulamento vengono rimosse.

È possibile abilitare o disabilitare l'incapsulamento globalmente per tutti i dispositivi durante il processo di gestione selezionando la casella di controllo **Abilita incapsulamento su tutti i prossimi dispositivi gestiti** nella pagina Rileva e gestisci nuovi dispositivi. L'incapsulamento è disabilitato per impostazione predefinita.



È inoltre possibile abilitare o disabilitare singolarmente l'incapsulamento di specifici dispositivi gestiti in qualunque momento accedendo alla pagina di riepilogo dei dispositivi, selezionando il dispositivo e facendo clic su **Azioni → Abilita incapsulamento** o **Azioni → Disabilita incapsulamento**.

Attenzione: Se l'incapsulamento è abilitato e XClarity Administrator non è più disponibile prima che la gestione di un dispositivo venga annullata, è necessario eseguire la procedura per disabilitare

l'incapsulamento al fine di stabilire la comunicazione con il dispositivo. Per le procedure di ripristino, vedere lenovoMgrAlert.mib file e Ripristino della gestione con un modulo CMM dopo un errore del server di gestione.

Nota: l'incapsulamento non è supportato su switch, dispositivi di storage, chassis e server non Lenovo.

Implementazione della conformità NIST SP 800-131A

Se è necessario rispettare la conformità NIST SP 800-131A, è possibile iniziare a progettare un ambiente completamente conforme tramite Lenovo XClarity Administrator.

Informazioni su questa attività

Nella pubblicazione speciale 800-131A (NIST SP 800-131A) del NIST (National Institute of Standards and Technology) vengono specificate le modalità di gestione delle comunicazioni sicure. Lo standard potenzia gli algoritmi e incrementa la lunghezza delle chiavi per aumentare la sicurezza. Lo standard NIST SP 800-131A richiede che le configurazioni degli utenti siano rigorosamente conformi allo standard.

Nota: I seguenti componenti di Flex System attualmente non supportano NIST SP 800-131A. Le comunicazioni tra XClarity Administrator o il modulo CMM e i seguenti componenti non sono conformi:
- Switch scalabile Flex System EN4023 10 Gb
- Switch Ethernet Flex System EN6131 40 Gb
- Switch SAN Flex System FC3171 8 Gb
- Switch scalabile SAN Flex System FC5022 16 Gb
- Switch InfiniBand Flex System IB6131

Nota: Quando per l'autenticazione viene utilizzato un provider di identità SAML, XClarity Administrator utilizza SHA-1 per firmare i metadati. L'utilizzo dell'algoritmo SHA-1 per le firme digitali non è conforme a NIST SP 800-131A.

Procedura

Per implementare la conformità NIST SP 800-131A, completare le seguenti operazioni.

Passo 1. Verificare che i dispositivi rispettino i seguenti criteri:
- Utilizzare Secure Sockets Layer (SSL) sul protocollo TLS v1.2.
- Utilizzare le funzioni di hash SHA-256 o più avanzate per le firme digitali e le funzioni di hash SHA-1 o più avanzate per le altre applicazioni.
- Utilizzare RSA-2048 o un metodo di crittografia ancora più sicuro oppure utilizzare la crittografia ECC (Elliptic Curve Cryptography) del NIST a 224 bit o superiore.
- Utilizzare la crittografia simmetrica approvata dal NIST con lunghezza delle chiavi di almeno 128 bit.
- Utilizzare i generatori di numeri casuali approvati dal NIST.
- Laddove possibile, supportare i meccanismi di scambio delle chiavi Diffie-Hellman o Elliptic Curve Diffie-Hellman.

Passo 2. Configurare le impostazioni di crittografia di Lenovo XClarity Administrator. Sono disponibili due impostazioni relative alla conformità NIST SP 800-131A:
- La *modalità SSL/TLS* specifica i protocolli da utilizzare per le comunicazioni sicure. XClarity Administrator supporta una configurazione **server e client TLS 1.2** per limitare il protocollo di crittografia a TLS 1.2 per XClarity Administrator e tutti i dispositivi gestiti.
- Se vengono implementate comunicazioni sicure, la *modalità crittografica* imposta la lunghezza delle chiavi di crittografia da utilizzare. È possibile impostare la modalità crittografica su **NIST SP 800-131A**. Tuttavia, potrebbe non essere possibile distribuire alcuni sistemi operativi tramite

XClarity Administrator, poiché alcuni programmi di installazione dei sistemi operativi non supportano le impostazioni limitate. Per supportare la distribuzione del sistema operativo, è possibile consentire le eccezioni per la distribuzione del sistema operativo.

Quando si modifica un'impostazione crittografica, XClarity Administrator esegue il provisioning delle nuove impostazioni su tutti i dispositivi gestiti e tenta di risolvere i nuovi certificati sui dispositivi selezionati.

Nota: Una volta modificate le impostazioni di crittografia, affinché le modifiche siano effettive e per ripristinare i servizi persi, è necessario riavviare manualmente XClarity Administrator (vedere Riavvio di XClarity Administrator).

Per ulteriori informazioni su queste impostazioni, vedere Configurazione delle impostazioni di crittografia sul server di gestione.

Passo 3. Utilizzare un browser Web che supporta il protocollo TLS1.2 e le funzioni di hashing SHA-256 e abilitare queste impostazioni nel browser Web.

Nota: Se si utilizza o si intende utilizzare certificati personalizzati o con firma esterna, tutti i certificati nella catena devono essere basati sulle funzioni di hash SHA-256.

Passo 4. Utilizzare i protocolli crittografati per tutte le comunicazioni. Non abilitare protocolli non crittografati, come Telnet, FTP e VNC per le comunicazioni remote con i dispositivi gestiti di XClarity Administrator.

Utilizzo di VMware Tools

Il pacchetto VMware Tools viene installato nel sistema operativo guest della macchina virtuale, quando si installa Lenovo XClarity Administrator in ambienti basati su VMware ESXi. Questo pacchetto fornisce una serie di strumenti VMware che supportano il backup e la migrazione ottimizzati delle appliance virtuali, preservando lo stato e la continuità delle applicazioni.

Per ulteriori informazioni sull'utilizzo di VMware Tools, vedere Utilizzo di VMware Tools Configuration Utility nel sito Web del centro documentazione di VMware vSphere.

Configurazione dell'accesso alla rete

Quando si configura per la prima volta Lenovo XClarity Administrator, è possibile configurare fino a due interfacce di rete. Inoltre, è necessario specificare quale interfaccia utilizzare per distribuire i sistemi operativi. Una volta completata la configurazione iniziale, è possibile modificare le impostazioni.

Prima di iniziare

Attenzione:

- La modifica dell'indirizzo IP di XClarity Administrator dopo la gestione dei dispositivi potrebbe determinare l'attivazione dello stato offline dei dispositivi in XClarity Administrator. Verificare che tutti i dispositivi risultino non gestiti prima di modificare l'indirizzo IP.
- È possibile abilitare o disabilitare il controllo degli indirizzi IP duplicati nella stessa sottorete, facendo clic sull'interruttore **Controllo dell'indirizzo IP duplicato**. L'opzione è disabilitata per impostazione predefinita. Quando l'opzione è abilitata, XClarity Administrator genera un avviso se si tenta di modificare l'indirizzo IP di XClarity Administrator o di gestire un dispositivo con lo stesso indirizzo IP di un altro dispositivo gestito o presente nella stessa sottorete.

  Nota: Se abilitato, XClarity Administrator esegue una scansione ARP per individuare i dispositivi IPv4 attivi nella stessa sottorete. Per evitare la scansione ARP, disabilitare **Controllo dell'indirizzo IP duplicato**.

- Quando si esegue XClarity Administrator come appliance virtuale, se l'interfaccia di rete per la rete di gestione è configurata per utilizzare il protocollo DHCP (Dynamic Host Configuration Protocol), l'indirizzo IP dell'interfaccia di gestione potrebbe cambiare alla scadenza del protocollo DHCP. Se l'indirizzo IP cambia, è necessario annullare la gestione di chassis, rack e server tower e quindi gestirli nuovamente. Per evitare questo problema, modificare l'interfaccia di gestione con un indirizzo IP statico oppure verificare che la configurazione del server DHCP sia impostata in modo che l'indirizzo DHCP sia basato su un indirizzo MAC o che il protocollo DHCP non scada.
- Se *non* si intende utilizzare XClarity Administrator per distribuire il sistema operativo o aggiornare i driver di dispositivo del sistema operativo, è possibile disabilitare i server Samba e Apache modificando l'interfaccia di rete per utilizzare l'opzione **rileva e gestisci solo l'hardware**. Tenere presente che il server di gestione viene riavviato una volta modificata l'interfaccia di rete.
- Quando si esegue XClarity Administrator come contenitore.
  - È possibile abilitare o disabilitare solo il controllo degli indirizzi IP duplicati, modificare i ruoli dell'interfaccia di rete e cambiare le impostazioni del proxy. Tutte le altre impostazioni di rete (come indirizzo IP, gateway e DNS) vengono definite nella configurazione del contenitore.
  - Verificare che sul sistema host sia impostata una rete macvlan.

Informazioni su questa attività

XClarity Administrator dispone di due interfacce di rete separate che possono essere definite in base all'ambiente, a seconda della topologia di rete implementata. Per le appliance virtuali, queste reti sono denominata eth0 ed eth1. Per i contenitori, è possibile scegliere nomi personalizzati.

- Se è presente solo un'interfaccia di rete (eth0):
  - L'interfaccia deve essere configurata per supportare il rilevamento dei dispositivi e la gestione (ad esempio, configurazione del server e aggiornamenti firmware). Deve essere in grado di comunicare con i moduli CMM e gli switch Flex di ogni chassis gestito, con il controller di gestione della scheda di base di ciascun server gestito e con ogni switch RackSwitch.
  - Se si intende acquistare gli aggiornamenti relativi a firmware e driver di dispositivo del sistema operativo mediante XClarity Administrator, almeno una delle interfacce di rete deve essere connessa a Internet, preferibilmente tramite un firewall. In caso contrario, è necessario importare gli aggiornamenti nel repository.
  - Se si desidera raccogliere i dati di servizio o utilizzare la notifica automatica dei problemi (come Call Home e Funzione Caricamento Lenovo), almeno una delle interfacce di rete deve essere collegata a Internet, preferibilmente tramite un firewall.
  - Se si intende distribuire le immagini del sistema operativo e aggiornare i driver di dispositivo del sistema operativo, l'interfaccia di rete deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzata per accedere al sistema operativo host.

    Nota: Se si implementa una rete separata per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo, è possibile configurare la seconda interfaccia di rete per il collegamento a questa rete invece che alla rete di dati. Tuttavia, se il sistema operativo di ciascun server non ha accesso alla rete di dati, è necessario configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host alla rete di dati, per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo
- Se sono presenti due interfacce di rete (eth0 e eth1):
  - La prima interfaccia di rete (in genere, l'interfaccia Eth0) deve essere collegata alla rete di gestione e configurata per supportare il rilevamento dei dispositivi e la gestione (come configurazione del server e aggiornamenti firmware). Deve essere in grado di comunicare con i moduli CMM e gli switch Flex di ogni chassis gestito, con il controller di gestione di ciascun server gestito e con ogni switch RackSwitch.

- La seconda interfaccia di rete (generalmente l'interfaccia eth1) può essere configurata per comunicare con una rete di dati interna, una rete di dati pubblica o entrambe.
- Se si intende acquistare gli aggiornamenti relativi a firmware e driver di dispositivo del sistema operativo mediante XClarity Administrator, almeno una delle interfacce di rete deve essere connessa a Internet, preferibilmente tramite un firewall. In caso contrario, è necessario importare gli aggiornamenti nel repository.
- Se si desidera raccogliere i dati di servizio o utilizzare la notifica automatica dei problemi (come Call Home e Funzione Caricamento Lenovo), almeno una delle interfacce di rete deve essere collegata a Internet, preferibilmente tramite un firewall.
- Se si intende distribuire le immagini del sistema operativo e aggiornare i driver di dispositivo, è possibile scegliere di utilizzare l'interfaccia eth1 o eth0. Tuttavia, l'interfaccia utilizzata deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzato per accedere al sistema operativo host.

  Nota: Se si implementa una rete separata per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo, è possibile configurare la seconda interfaccia di rete per il collegamento a questa rete invece che alla rete di dati. Tuttavia, se il sistema operativo di ciascun server non ha accesso alla rete di dati, è necessario configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host alla rete di dati, per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo

Nella seguente tabella sono riportate le possibili configurazioni per le interfacce di rete di XClarity Administrator in base al tipo di topologia di rete implementata nell'ambiente. Utilizzare questa tabella per determinare le modalità di definizione di ciascuna interfaccia di rete.

Tabella 2. Ruolo di ciascuna interfaccia di rete basata sulla topologia di rete

Topologia di rete	**Ruolo dell'interfaccia 1 (eth0)**	**Ruolo dell'interfaccia 2 (eth1)**
Rete convergente (rete di dati e gestione con supporto per la distribuzione del sistema operativo e degli aggiornamenti dei driver di dispositivo del sistema operativo)	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia • Distribuzione sistema operativo • Aggiornamenti dei driver di dispositivo del sistema operativo	Nessuna
Rete di gestione separata con supporto per la distribuzione del sistema operativo, degli aggiornamenti dei driver di dispositivo del sistema operativo e della rete di dati	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia • Distribuzione sistema operativo • Aggiornamenti dei driver di dispositivo del sistema operativo	Rete di dati • Nessuna

Tabella 2. Ruolo di ciascuna interfaccia di rete basata sulla topologia di rete (continua)

Topologia di rete	Ruolo dell'interfaccia 1 (eth0)	Ruolo dell'interfaccia 2 (eth1)
Rete di gestione separata e rete di dati con supporto per la distribuzione del sistema operativo e degli aggiornamenti dei driver di dispositivo	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia	Rete di dati • Distribuzione sistema operativo • Aggiornamenti dei driver di dispositivo del sistema operativo
Rete di gestione separata e rete di dati senza supporto per la distribuzione del sistema operativo e degli aggiornamenti dei driver di dispositivo	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia	Rete di dati • Nessuna
Rete di sola gestione (la distribuzione del sistema operativo e dei driver di dispositivo del sistema operativo non è supportata)	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia	Nessuna

Per ulteriori informazioni sulle interfacce di rete di XClarity Administrator, come le limitazioni degli indirizzi IPv6, vedere Considerazioni sulla rete nella XClarity Administrator documentazione online.

Procedura

Per configurare l'accesso alla rete, completare la seguente procedura.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Accesso alla rete**. Vengono visualizzate le impostazioni di rete correnti.

Passo 2. Facoltativamente è possibile abilitare il controllo degli indirizzi IP duplicati nella stessa sottorete, facendo clic sull'interruttore **Controllo dell'indirizzo IP duplicato**.

Quando l'opzione è abilitata, XClarity Administrator genera un avviso se si tenta di modificare l'indirizzo IP di XClarity Administrator o di gestire un dispositivo con lo stesso indirizzo IP di un altro dispositivo gestito o presente nella stessa sottorete.

Passo 3. Fare clic su **Modifica accesso alla rete** per visualizzare la pagina Modifica accesso alla rete.

Passo 4. Se si intende distribuire i sistemi operativi e aggiornare i driver di dispositivo del sistema operativo mediante XClarity Administrator, scegliere l'interfaccia di rete da utilizzare per la gestione dei sistemi operativi.

- Se è definita solo un'interfaccia per XClarity Administrator, scegliere se utilizzarla solo per rilevare e gestire l'hardware oppure anche per gestire i sistemi operativi.
- Se sono definite due interfacce per XClarity Administrator (Eth0 ed Eth1), scegliere quella da utilizzare per gestire i sistemi operativi. Se si sceglie "Nessuno", *non* sarà possibile distribuire le immagini del sistema operativo o aggiornare i driver di dispositivo del sistema operativo dei server gestiti da XClarity Administrator.

Passo 5. (XClarity Administrator solo come appliance virtuale) Modificare le impostazioni IP.

a. Per la prima interfaccia, specificare l'indirizzo IPv4, l'indirizzo IPv6 o entrambi.

- **IPv4**. È necessario assegnare un indirizzo IPv4 all'interfaccia. È possibile scegliere di utilizzare un indirizzo IP assegnato staticamente oppure ottenere un indirizzo IP da un server DHCP.
- **IPv6**. Facoltativamente, è possibile assegnare un indirizzo IPv6 all'interfaccia mediante uno dei seguenti metodi di assegnazione:
  - Utilizza indirizzo IP assegnato in modo statico
  - Utilizza la configurazione dell'indirizzo senza stato (DHCPv6)
  - Utilizza configurazione automatica dell'indirizzo senza stato

  Nota: Per informazioni sulle limitazioni degli indirizzi IPv6, vedere Limitazioni della configurazione IPv6 nella documentazione online di XClarity Administrator.

b. Se è disponibile una seconda interfaccia, specificare l'indirizzo IPv4, l'indirizzo IPv6 o entrambi.

Nota: Gli indirizzi IP assegnati a questa interfaccia devono essere in una sottorete diversa da quella degli indirizzi IP assegnati alla prima interfaccia. Se si decide di utilizzare DHCP per assegnare indirizzi IP per entrambe le interfacce (Eth0 e Eth1), il server DHCP non deve assegnare la stessa sottorete per gli indirizzi IP delle due interfacce.

- **IPv4**. È possibile scegliere di utilizzare un indirizzo IP assegnato staticamente oppure ottenere un indirizzo IP da un server DHCP.
- **IPv6**. Facoltativamente, è possibile assegnare un indirizzo IPv6 all'interfaccia mediante uno dei seguenti metodi di assegnazione:
  – Utilizza indirizzo IP assegnato in modo statico
  – Utilizza la configurazione dell'indirizzo senza stato (DHCPv6)
  – Utilizza configurazione automatica dell'indirizzo senza stato

c. Specificare il gateway predefinito.

Se si specifica un gateway predefinito, deve essere un indirizzo IP valido e utilizzare la stessa maschera di rete (la stessa sottorete) dell'indirizzo IP per una delle interfacce di rete (Eth0 o Eth1). Se si utilizza una singola interfaccia, il gateway predefinito deve essere nella stessa sottorete dell'interfaccia di rete.

Se una delle due interfaccia utilizza DHCP per ottenere l'indirizzo IP, anche il gateway predefinito utilizza DHCP. Per immettere manualmente un indirizzo gateway predefinito che sovrascriva quello ricevuto dal server DHCP, selezionare la casella di controllo **Sovrascrivi gateway**.

Suggerimenti:

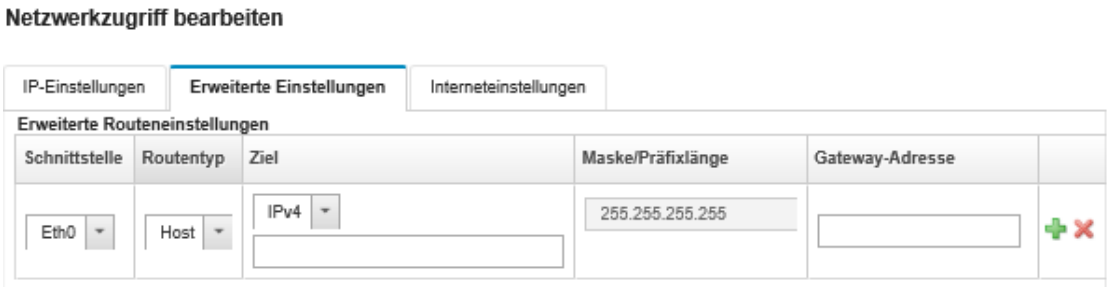
- Verificare che il gateway corrisponda a una sottorete delle interfacce di rete. Il gateway predefinito viene impostato automaticamente tramite questa interfaccia di rete.
- Per tornare a un gateway fornito da DHCP, deselezionare la casella di controllo **Sovrascrivi gateway**.

ATTENZIONE:
Se si sceglie di ignorare il gateway, immettere l'indirizzo gateway corretto. In caso contrario, questo server di gestione non sarà raggiungibile e non vi sarà alcun modo di eseguire il log in remoto per correggerlo.

d. Fare clic su **Salva impostazioni IP**.

Passo 6. (XClarity Administrator solo come appliance virtuale) Modificare facoltativamente le impostazioni avanzate.

a. Fare clic sulla scheda **Instradamento avanzato**.



b. Specificare una o più voci di instradamento nella tabella **Impostazioni instradamento avanzate** per l'utilizzo da parte di questa interfaccia.

Per definire una o più voci di instradamento, attenersi alla procedura descritta di seguito.
1. Scegliere l'interfaccia.
2. Specificare il tipo di instradamento, che può essere un instradamento a un altro host o a una rete.
3. Specificare l'indirizzo di rete o l'host di destinazione a cui si esegue l'indirizzamento dell'instradamento.

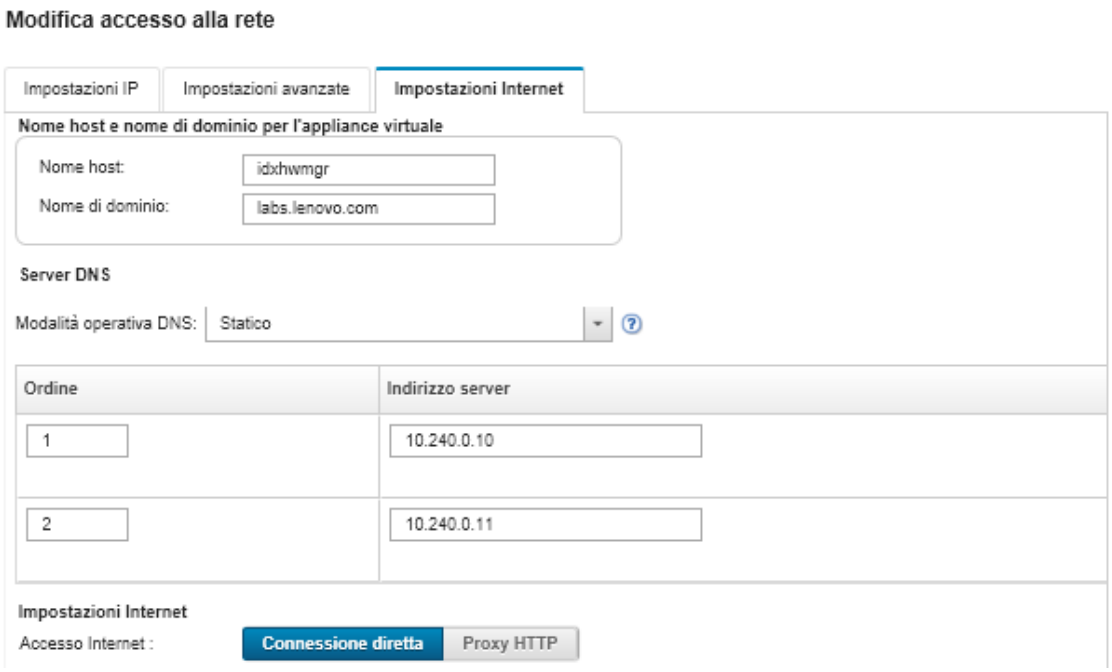
4. Specificare la maschera di sottorete per l'indirizzo di destinazione.
5. Specificare l'indirizzo gateway a cui verranno indirizzati i pacchetti.

c. Fare clic sulla scheda **Salva instradamento avanzato**.

Passo 7. Facoltativamente, modificare le impostazioni DNS e proxy.

Quando XClarity Administrator è configurato come un contenitore, dall'interfaccia Web è possibile modificare solo le impostazioni del proxy. Le impostazioni DNS vengono definite nel contenitore.

a. Fare clic sulla scheda **DNS e proxy**.



b. Specificare il nome host e il nome di dominio da utilizzare per XClarity Administrator.

c. Selezionare la modalità operativa DNS. Può essere **Statica** o **DHCP**.

Attenzione: È necessario riavviare il server di gestione quando si modifica la modalità operativa DNS.

Nota: Se si sceglie di utilizzare un server DHCP per ottenere l'indirizzo IP, eventuali modifiche apportate ai campi **Server DNS** verranno sovrascritte al successivo rinnovo del lease DHCP da parte di XClarity Administrator.

d. Specificare l'indirizzo IP di uno o più server DNS (Domain Name System) da utilizzare e l'ordine di priorità per ciascuno di essi.

e. Specificare se accedere a Internet utilizzando una connessione diretta o un proxy HTTP (se XClarity Administrator ha accesso a Internet).

Nota: Se si utilizza un proxy HTTP, verificare che siano rispettati i seguenti requisiti.
- Accertarsi che il server proxy sia configurato per utilizzare l'autenticazione di base.
- Accertarsi che il server proxy sia configurato come proxy non ricevitore.
- Accertarsi che il server proxy sia configurato come proxy di inoltro.
- Accertarsi che i bilanciamenti del carico siano configurati in modo da mantenere sessioni con un solo server proxy e non scambiandole.

Se si sceglie di utilizzare un proxy HTTP, compilare i campi obbligatori:
1. Specificare il nome host e la porta del server proxy.

2. Scegliere se utilizzare l'autenticazione e specificare il nome utente e la password, se necessario.
3. Specificare l'URL del test proxy.
4. Fare clic su **Test proxy** per verificare che le impostazioni proxy siano configurati e funzionino correttamente.

f. Fare clic su **Salva DNS e proxy**.

g. È possibile eseguire il push del nome FQDN (Fully-Qualified Domain Name) e delle informazioni DNS del server di gestione XClarity Administrator ai server gestiti con IMM2, XCC e XCC2, in modo che i server gestiti possano trovare il server di gestione utilizzando queste informazioni.

1. Fare clic su **Esegui push di FQDN/DNS su BMC**.
2. Scegliere come gestire le voci DNS esistenti nel controller di gestione della scheda di base.
   - Mantenere le voci DNS esistenti e aggiungere le voci DNS del server di gestione nel successivo slot disponibile.
   - Sostituire tutte le voci DNS esistenti con le voci DNS del server di gestione.
3. Digitare **SÌ** nel campo di modifica.
4. Fare clic su **Applica**.

Viene creato un processo per eseguire questa operazione. È possibile monitorare l'avanzamento del processo dalla scheda **Monitoraggio → Processi**. Se il processo non è stato completato correttamente, fare clic sul relativo collegamento per visualizzare i dettagli sul processo (vedere).

È inoltre possibile rimuovere le informazioni DNS e FQDN del server di gestione dai server gestiti con IMM2, XCC e XCC2 facendo clic su **Rimuovi FQDN/DNS da BMC**. È possibile scegliere di mantenere altre voci DNS esistenti, rimuovere tutte le voci DNS oppure rimuovere solo le voci che corrispondono alle informazioni del server di gestione.

Passo 8. Fare clic su **Riavvia** per riavviare il server di gestione.

Passo 9. Fare clic su **Test della connessione** per verificare le impostazioni di rete.

Impostazione di data e ora

È possibile impostare la data e l'ora di Lenovo XClarity Administrator.

Prima di iniziare

È necessario utilizzare almeno uno (e fino a quattro) server NTP (Network Time Protocol) per sincronizzare i timestamp di tutti gli eventi ricevuti dai dispositivi gestiti con XClarity Administrator.

Suggerimento: il server NTP deve essere accessibile sulla rete di gestione (in genere, l'interfaccia Eth0). Valutare la possibilità di configurare il server NTP sull'host in cui XClarity Administrator è in esecuzione.

Se si modifica l'ora sul server NTP, la sincronizzazione di XClarity Administrator con la nuova ora potrebbe richiedere tempo.

Attenzione: L'appliance virtuale XClarity Administrator e il relativo host devono essere impostati per sincronizzarsi con la stessa origine dell'ora, in modo da impedire l'errata sincronizzazione oraria tra XClarity Administrator e il relativo host. In genere, l'host è configurato per sincronizzarsi con l'ora delle rispettive appliance virtuali. Se XClarity Administrator è impostato per sincronizzarsi con un'origine differente rispetto

all'host, è necessario disabilitare la sincronizzazione oraria dell'host tra l'appliance virtuale XClarity Administrator e il rispettivo host.

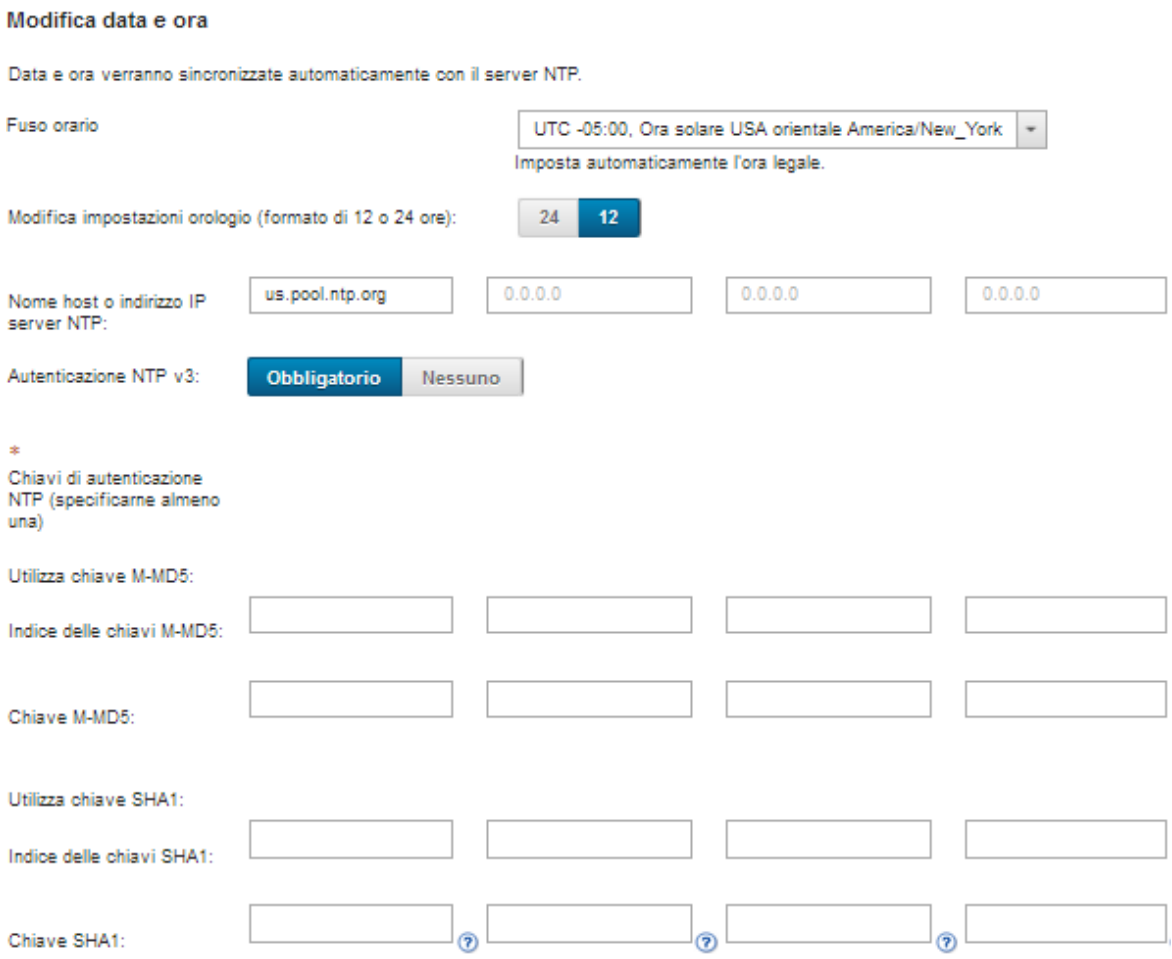
- Per ESXi, seguire le istruzioni sulla VMware - Pagina Web sulla disabilitazione della sincronizzazione dell'ora.
- Per Hyper-V di Hyper-V Manager, fare clic con il pulsante destro del mouse sulla macchina virtuale XClarity Administrator e quindi fare clic su **Impostazioni**. Nella finestra di dialogo, fare clic su **Gestione > Servizi di integrazione** nel riquadro di navigazione e quindi deselezionare **Sincronizzazione ora**.

Procedura

Per l'impostazione della data e dell'ora di XClarity Administrator, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Data e ora**. Viene visualizzata la pagina Data e ora. Questa pagina mostra la data e l'ora correnti per XClarity Administrator.

Passo 2. Fare clic su **Modifica data e ora** per visualizzare la pagina Modifica data e ora



Passo 3. Compilare la finestra di dialogo Data e ora.

1. Scegliere il fuso orario in cui si trova l'host per XClarity Administrator.

   Se il fuso orario selezionato osserva l'ora legale, l'ora viene automaticamente regolata di conseguenza.

2. Scegliere di utilizzare un formato a 12 o 24 ore.
3. Specificare il nome host o l'indirizzo IP di ciascun server NTP nella rete. È possibile definire fino a quattro server NTP.

4. Selezionare **Richiesta** per abilitare l'autenticazione NTP v3 oppure **Nessuno** per utilizzare l'autenticazione NTP v1 tra XClarity Administrator e i server NTP in rete.

   È possibile utilizzare l'autenticazione v3 se i moduli CMM di Flex System e i controller di gestione della scheda di base utilizzano firmware che richiedono l'autenticazione v3 e se l'autenticazione NTP v3 è richiesta tra XClarity Administrator e uno o più dei server NTP nella rete

5. Se si abilita l'autenticazione NTP v3, impostare la chiave di autenticazione e l'indice per ciascun server NTP applicabile. È possibile specificare una chiave M-MD5, SHA1 o entrambe. Se sono state specificate le chiavi M-MD5 e SHA1, XClarity Administrator effettua il push della chiave M-MD5 o SHA1 ai moduli CMM di Flex System e ai controller di gestione che la supportano. XClarity Administrator utilizza la chiave per eseguire l'autenticazione con il server NTP.
   - Per la chiave M-MD5, specificare una stringa ASCII che include solo lettere minuscole e maiuscole (a-z, a-Z), cifre (0-9) e i seguenti caratteri speciali @#.
   - Per la chiave SHA1, specificare una stringa ASCII di 40 caratteri, includendo esclusivamente numeri tra 0 e 9 e lettere tra a e f.
   - L'indice della chiave specificata e la chiave di autenticazione devono corrispondere all'ID della chiave e alla password impostati nel server NTP. Ad esempio, se l'indice chiave della chiave SHA1 immessa nel server NTP è 5, anche l'indice della chiave specificato della chiave SHA1 di XClarity Administrator è 5. Per informazioni sull'impostazione dell'ID della chiave e della password, vedere la documentazione del server NTP.
   - È necessario specificare la chiave per ciascun server NTP che utilizza l'autenticazione v3, anche se due o più server NTP utilizzano la stessa chiave.
   - Se si abilita l'autenticazione v3, ma non vengono fornite una chiave di autenticazione e l'indice per un server NTP, l'autenticazione v1 viene utilizzata per impostazione predefinita.
   - Se sono stati specificati più server NTP, i server NTP devono disporre tutti dell'autenticazione v3 o v1. Un insieme di server NTP con autenticazione v3 e v1 mista non è supportato.
   - Se sono stati specificati più server NTP con autenticazione v3, gli indici di chiave devono essere univoci se le chiavi non sono identiche. Ad esempio, i server NTP 1 e 2 non possono avere l'indice di chiave SHA1 del server 1, se le chiavi SHA1 del server NTP 1 e 2 sono differenti. È necessario riconfigurare uno dei server NTP per accettare la chiave con un indice di chiave differente rispetto all'altro server NTP. In caso contrario, l'ultima chiave definita associata a un indice di chiave verrà configurata per tutti i server NTP con lo stesso indice di chiave.

Passo 4. Fare clic su **Salva**.

Impostazioni preferenze inventario

È possibile impostare le preferenze dell'inventario per i dispositivi gestiti, incluse le proprietà da utilizzare per visualizzare il nome del dispositivo.

Procedura

Completare le seguenti operazioni per configurare le preferenze dell'inventario per i dispositivi gestiti.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Preferenze inventario**. Verrà visualizzata la pagina "Preferenze inventario".

Passo 2. Selezionare la proprietà da utilizzare per il nome del dispositivo visualizzato nell'interfaccia utente di Lenovo XClarity Administrator. È possibile selezionare una delle seguenti proprietà:
   - **Sequenza predefinita (predefinito)**

- **Nome definito dall'utente**
- **Nome host DNS**
- **Nome host**
- **Indirizzo IPv4**
- **Numero di serie**

Se **Sequenza predefinita** è selezionata, il nome del dispositivo visualizzato viene scelto in base alla sequenza di proprietà nell'elenco precedente. Ad esempio, se un dispositivo dispone di un nome definito dall'utente, tale nome viene visualizzato. Se un dispositivo non dispone di un nome definito dall'utente, viene visualizzato il nome host DNS. Se un dispositivo non dispone di un nome definito dall'utente o di un nome host DNS, viene visualizzato il nome host.

Nota: Se si seleziona un valore diverso rispetto a quello predefinito viene modificato il nome visualizzato nell'interfaccia utente di Lenovo XClarity Administrator per tutti i dispositivi con la proprietà selezionata. Il nome definito dall'utente assegnato al dispositivo non varia.

Passo 3. Facoltativamente, fare clic su **Abilita** per scegliere di ordinare le griglie (tabelle) utilizzando il valore selezionato per il nome del dispositivo.

Passo 4. Selezionare la preferenza dell'ordine di numerazione dei rack, dal primo all'ultimo (ad esempio, 1-52) o dall'ultimo al primo (ad esempio, 52-1).

Nota: La modifica della preferenza dell'ordine numerico non cambia la posizione di un dispositivo nel rack.

Passo 5. Fare clic su **Applica**.

Al termine

È possibile impostare le preferenze delle soglie per la generazione di un avviso e di un evento quando un determinato valore, come la durata di un'unità SSD di un server ThinkSystem o ThinkServer supera un livello di avvertenza o critico (vedere Impostazione delle preferenze delle soglie per la generazione di eventi e avvisi).

Impostazione delle preferenze delle soglie per la generazione di eventi e avvisi

È possibile impostare le preferenze delle soglie per la generazione di un avviso e di un evento quando un determinato valore, come la durata di un'unità SSD di un server ThinkSystem o ThinkServer, supera un livello di avvertenza o criticità.

Procedura

Per inoltrare specifici file di servizio al fornitore di servizi, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Monitoraggio → Avvisi** per visualizzare la pagina Avvisi.

Passo 2. Fare clic sull'icona **Impostazioni di soglia** () per visualizzare la finestra di dialogo Impostazioni di soglia.

Passo 3. Modificare le soglie di avvertenza o criticità per la durata residua delle unità SSD dei server ThinkSystem e ThinkServer.

La durata rimanente delle unità SSD viene calcolata utilizzando i contatori SMART del fornitore. I valori predefiniti sono 30% per la soglia di avvertenza e 20% per la soglia critica.

Passo 4. Selezionare l'interruttore **Abilitato** per generare un avviso e un evento quando viene raggiunta ciascuna soglia.

Passo 5. Fare clic su **Applica**.

Configurazione dell'invio di notifiche automatiche dei problemi al Supporto Lenovo (Call Home)

È possibile creare un server d'inoltro di servizio in grado di inviare automaticamente dati di servizio per un dispositivo gestito a Supporto Lenovo mediante la funzione Call Home quando determinati eventi che richiedono assistenza, come una memoria irrecuperabile, vengono ricevuti da specifici dispositivi gestiti, affinché il problema possa essere risolto. Il servizio inoltrato viene denominato "Call Home predefinito".

Lenovo è impegnata nella sicurezza. Quando abilitato, contattare Call Home Centro assistenza clienti Lenovo quando un dispositivo riporta un guasto hardware o quando si sceglie di avviare una Call Home manuale. I dati di servizio che vengono in genere caricati manualmente sul supporto Lenovo vengono automaticamente inviati al Centro assistenza clienti Lenovo su HTTPS mediante TLS 1.2 o versione successiva. I dati relativi all'azienda non vengono mai trasmessi. L'accesso ai dati di servizio nel Centro assistenza clienti Lenovo è limitato al personale di assistenza autorizzato.

Prima di iniziare

Attenzione: È necessario accettare l'Informativa sulla privacy di Lenovo prima di poter trasferire i dati al supporto Lenovo.

Accertarsi che tutte le porte richieste da Lenovo XClarity Administrator (incluse le porte richieste per Call Home) siano disponibili prima di abilitare Call Home. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.

Accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti da Call Home. Per informazioni sui firewall, vedere Firewall e server proxy nella documentazione online di XClarity Administrator.

Se XClarity Administrator accede a Internet con un proxy HTTP, accertarsi che il server proxy sia configurato per l'utilizzo dell'autenticazione di base e come proxy non ricevitore. Per ulteriori informazioni sulla configurazione del proxy, vedere Configurazione dell'accesso alla reteConfigurazione dell'accesso alla rete nella documentazione online di XClarity Administrator.

Una volta configurato Call Home, il server d'inoltro di servizio **Lenovo Call Home predefinito** viene aggiunto alla pagina Server d'inoltro di servizio. È possibile modificare questo server d'inoltro di servizio per configurare impostazioni aggiuntive, quali i dispositivi associati a questo server d'inoltro di servizio. Tutti i dispositivi vengono associati per impostazione predefinita. Se non viene specificato alcun dispositivo, Call Home *non* invierà le notifiche dei problemi al supporto Lenovo.

Informazioni su questa attività

Un *server d'inoltro di servizio* definisce le informazioni sulla destinazione dell'invio dei file di dati di servizio quando si verifica un evento che richiede assistenza. È possibile definire fino a 50 server d'inoltro di servizio.

- **Se un server d'inoltro di servizio Call Home non è configurato**, è possibile aprire manualmente un ticket di assistenza e inviare file di servizio a Centro assistenza clienti Lenovo seguendo le istruzioni fornite nel Pagina Web per la richiesta di un nuovo servizio. Per informazioni sulla raccolta e sul download di file di servizio, vedere Download dei file di diagnostica di XClarity Administrator e Raccolta e download dei file di diagnostica per un dispositivo nella documentazione online di XClarity Administrator.
- **Se un server d'inoltro di servizio Call Home è configurato ma non abilitato**, è possibile aprire *manualmente* un ticket di assistenza mediante la funzione Call Home per raccogliere e trasferire file di servizio al Centro assistenza clienti Lenovo in qualsiasi momento. Per ulteriori informazioni, vedere Apertura di un ticket di assistenza nella documentazione online di XClarity Administrator.

- **Se un server d'inoltro di servizio Call Home è configurato e abilitato**, XClarity Administrator raccoglie *automaticamente* i dati di servizio, apre un ticket di assistenza e trasferisce i file di servizio al Centro assistenza clienti Lenovo quando si verifica un evento che richiede assistenza per la risoluzione del problema.

  Importante: Quando si abilita un server d'inoltro di servizio Call Home in Lenovo XClarity Administrator, Call Home è disabilitata in ogni dispositivo gestito, al fine di evitare la creazione di record dei problemi duplicati. Se non si intende più utilizzare XClarity Administrator per gestire i dispositivi o si intende disabilitare Call Home in XClarity Administrator, è possibile riabilitare Call Home in tutti i dispositivi gestiti da XClarity Administrator anziché riabilitare Call Home per ogni singolo dispositivo in un secondo momento. Per informazioni su come riabilitare Call Home su tutti i dispositivi gestiti quando il server d'inoltro di servizio per Call Home è disabilitato, vedere Riabilitazione di call home su tutti i dispositivi gestiti nella documentazione online di XClarity Administrator.Per i server con XCC2, XClarity Administrator salva i dati di servizio in due file nel repository.

  – **File di servizio**. (.zip) Questo file contiene informazioni su servizio e inventario in un formato facilmente leggibile. Questo file viene inviato automaticamente al Centro assistenza clienti Lenovo quando si verifica un evento di manutenzione.
  – **File di debug**. (.tzz) Il file contiene tutte le informazioni sul servizio, l'inventario e i log di debug per l'utilizzo da parte del supporto Lenovo. È possibile inviare manualmente questo file al supporto Lenovo, se sono necessarie ulteriori informazioni per risolvere un problema.

  Per altri dispositivi, XClarity Administrator salva i dati di servizio (tra cui informazioni su servizio, inventario e log di debug) in un singolo file di servizio nel repository. Questo file viene inviato al Centro assistenza clienti Lenovo quando si verifica un evento di manutenzione.

  Sebbene XClarity Administrator supporti la funzionalità Call Home per i dispositivi ThinkAgile e ThinkSystem, il controller di gestione della scheda di base per alcuni dispositivi ThinkAgile e ThinkSystem non include il supporto Call Home. Pertanto, non è possibile abilitare o disabilitare Call Home su questi dispositivi. Call Home può essere abilitato solo per i dispositivi al livello di XClarity Administrator.

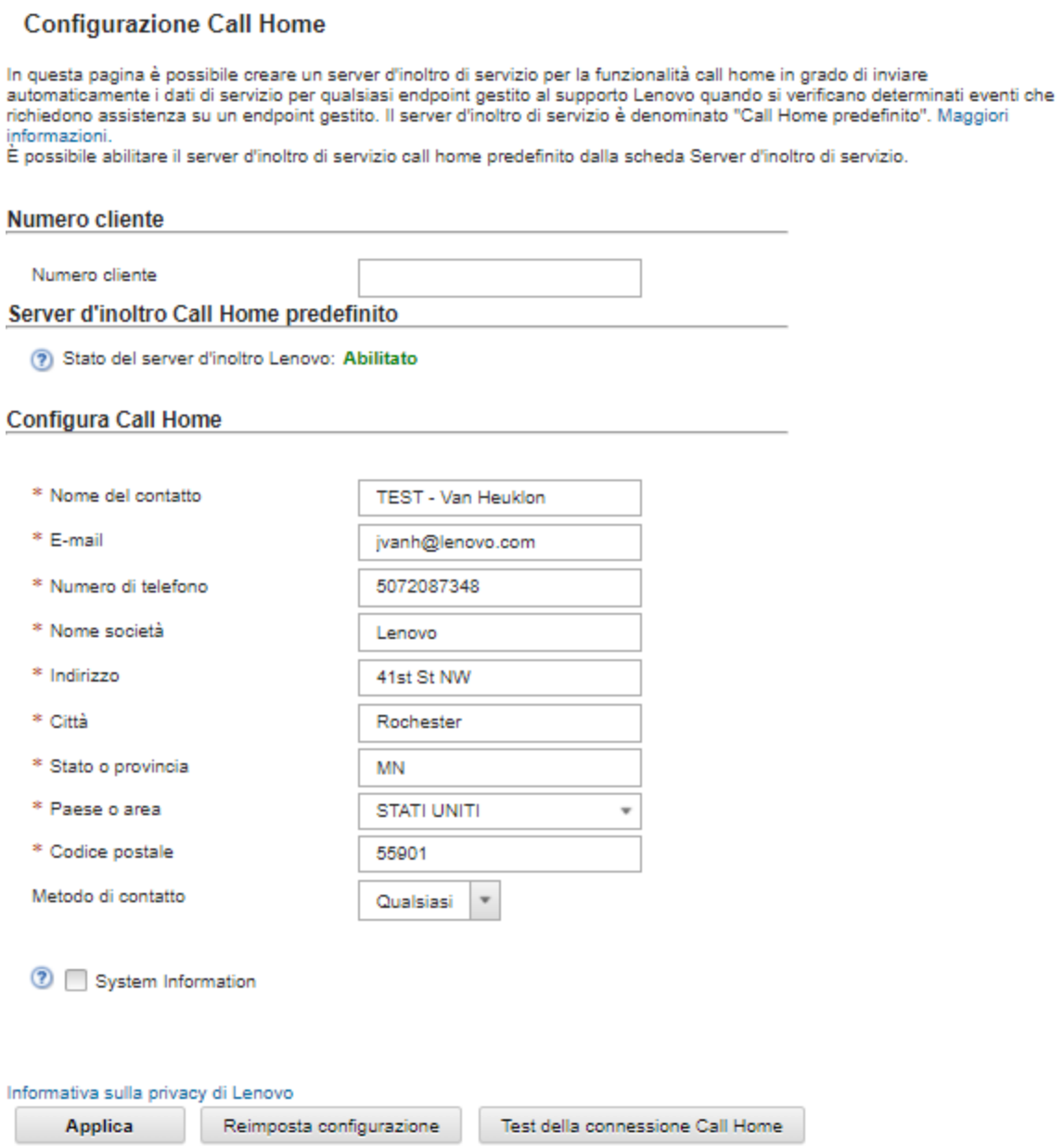
  Call Home viene eliminato per gli eventi ripetuti per qualsiasi dispositivo, se un ticket di assistenza è aperto per quell'evento su quel dispositivo. Call Home viene eliminato anche per gli eventi simili di qualsiasi dispositivo ThinkAgile e ThinkSystem, se un ticket di assistenza è aperto per un evento su quel dispositivo. Gli eventi ThinkAgile e ThinkSystem sono formati da stringhe di 16 caratteri nel seguente formato *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx* (ad esempio, `806F010D0401FFFF`). Gli eventi sono simili se hanno lo stesso tipo di lettura, tipo di sensore e ID entità. Ad esempio, se un ticket di assistenza è aperto per l'evento 806F010D0401FFFF su uno specifico dispositivo ThinkAgile o ThinkSystem, tutti gli eventi che si verificano su tale dispositivo con ID evento del tipo `xx6F01`*xx*`04`*xxxxxx*, dove *x* è un qualsiasi carattere alfanumerico, vengono eliminati.

  Per informazioni sulla visualizzazione dei ticket di assistenza aperti automaticamente da un server d'inoltro di servizio Call Home, vedere Visualizzazione di ticket di assistenza e stato nella documentazione online di XClarity Administrator.

Procedura

Completare le seguenti operazioni per configurare un servizio inviato per Call Home.

- Configurare Call Home per tutti i dispositivi gestiti (correnti e futuri):
  1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**.
  2. Fare clic su **Configurazione Call Home** nel riquadro di navigazione sinistro per visualizzare la pagina Configurazione Call Home.



3. (Facoltativo) Specificare il numero cliente Lenovo predefinito da utilizzare quando si segnalano i problemi con XClarity Administrator.

   Suggerimento: il numero cliente è indicato nell'e-mail di abilitazione ricevuta al momento dell'acquisto di Lenovo XClarity Pro.
4. Compilare le informazioni di contatto e posizione.
5. Selezionare il metodo preferito per essere contattati dal supporto Lenovo.
6. (Facoltativo) compilare le informazioni di sistema.
7. Fare clic su **Applica**.

   Verrà creato un Call Home server d'inoltro di servizio denominato "Call Home predefinito" per tutti i dispositivi gestiti utilizzando le informazioni di contatto specificate.
8. Abilitare e testare il server d'inoltro di servizio "Call Home predefinito".

a. Fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro per visualizzare la pagina Server d'inoltro di servizio.
b. Selezionare **Abilita** nella colonna **Stato** per il server d'inoltro di servizio "Call Home predefinito".
c. Selezionare il server d'inoltro di servizio "Call Home predefinito" e fare clic su **Test server d'inoltro di servizio** per generare un evento di test per il server d'inoltro di servizio e verificare che XClarity Administrator sia in grado di comunicare con il centro di assistenza Lenovo.

   Per monitorare l'avanzamento del test, fare clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator.

   Nota: Per poter essere testato, il server d'inoltro di servizio deve essere abilitato

- Configurare Call Home per i dispositivi gestiti specifici:
  1. Dalla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**.
  2. Fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro per visualizzare la pagina Server d'inoltro di servizio.
  3. Fare clic sull'icona **Crea server d'inoltro di servizio** ( ) per visualizzare la finestra di dialogo "Nuovo server d'inoltro di servizio".
  4. Fare clic sulla scheda **Generale**.

     a. Selezionare **Call Home** come server d'inoltro di servizio:
     b. Immettere il nome del server d'inoltro di servizio e una descrizione.
     c. Specificare il numero di tentativi di notifica automatici. Il valore predefinito è 2.
     d. Specificare il numero minimo di minuti tra i tentativi. Il valore predefinito è 2.
     e. (Facoltativo) Fare clic su **Ispezione dati di servizio necessaria** se si desidera controllare i file dei dati di servizio prima che vengano trasferiti e, facoltativamente, specificare l'indirizzo e-mail del contatto a cui inviare una notifica quando sarà necessario controllare i file di servizio.
  5. Fare clic sulla scheda **Specifico** e compilare le informazioni di sistema e di contatto.

     Suggerimento: per utilizzare le stesse informazioni di contatto e posizione configurate nella pagina di configurazione di Call Home, selezionare **Configurazione generale** nel menu a discesa **Configurazione**.
  6. Fare clic sulla scheda **Dispositivi** e selezionare i dispositivi gestiti e i gruppi di risorse per i quali si desidera che il server d'inoltro di servizio inoltri i file di servizio.

Suggerimento: per inoltrare i file di servizio per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i dispositivi**.

7. Fare clic su **Crea**. Il server d'inoltro di servizio viene aggiunto alla pagina Assistenza e supporto.
8. Nella pagina Server d'inoltro di servizio, selezionare **Abilita** nella colonna **Stato** per abilitare il server d'inoltro di servizio.
9. Selezionare il server d'inoltro di servizio e fare clic su **Test server d'inoltro di servizio** per generare un evento di test per il server d'inoltro di servizio e verificare che XClarity Administrator sia in grado di comunicare con il centro di assistenza Lenovo.

   Per monitorare l'avanzamento del test, fare clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator.

   Nota: Per poter essere testato, il server d'inoltro di servizio deve essere abilitato.

Al termine

Dalla pagina Assistenza e supporto è inoltre possibile procedere come segue:

- Se l'opzione **Ispezione dati di servizio necessaria** è selezionata ed è stato ricevuto un evento che richiede assistenza da uno dei dispositivi gestiti associati al server d'inoltro di servizio, è necessario controllare i file di servizio prima che vengano inoltrati al fornitore di servizi. Per ulteriori informazioni, vedere Trasferimento dei file di diagnostica al supporto Lenovo nella documentazione online di XClarity Administrator.
- Determinare se Call Home è abilitato o disabilitato in un dispositivo gestito facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro e verificando lo stato nella colonna **Call Home Stato**.

  Suggerimento: se "Stato sconosciuto" viene visualizzato nella colonna **Call Home Stato**, aggiornare il browser Web per visualizzare lo stato corretto.
- Definire le informazioni di contatto e posizione di supporto per uno specifico dispositivo gestito facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro, selezionando il dispositivo e quindi facendo clic sull'icona **Crea profilo di contatto** ( ) o sull'icona **Modifica profilo contatto** ( ). Le informazioni di contatto e posizione per il dispositivo gestito sono incluse nel ticket di assistenza che Call Home invia al Centro assistenza clienti Lenovo. Se vengono specificate informazioni di contatto e posizione univoche per un dispositivo gestito, verranno incluse nel ticket di assistenza. In caso contrario, verranno utilizzate informazioni generiche specificate per la configurazione XClarity Administrator Call Home (nella pagina **Call Home Configurazione** o **Server d'inoltro di servizio**). Per ulteriori informazioni, vedere Centro assistenza clienti Lenovo. Per ulteriori informazioni, vedere Definizione dei contatti di supporto per un dispositivo nella documentazione online di XClarity Administrator.
- Per visualizzare i ticket di assistenza inviati a Centro assistenza clienti Lenovo, fare clic su **Stato ticket di assistenza** nel riquadro di navigazione sinistro. In questa pagina sono elencati i ticket di assistenza aperti automaticamente o manualmente da un server d'inoltro di servizio Call Home, lo stato e i file di servizio trasmessi al Centro assistenza clienti Lenovo. Per ulteriori informazioni, vedere Visualizzazione di ticket di assistenza e stato nella documentazione online di XClarity Administrator.
- Raccogliere i dati di servizio per uno specifico dispositivo facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro, selezionando il dispositivo e quindi facendo clic sull'icona **Raccogli dati di servizio** ( ). Per ulteriori informazioni, vedere Raccolta e download dei file di diagnostica per un dispositivo nella documentazione online di XClarity Administrator.
- Aprire manualmente un ticket di assistenza nel Centro assistenza clienti Lenovo, raccogliere i dati di servizio per uno specifico dispositivo e inviarli al Centro assistenza clienti Lenovo facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro, selezionando il dispositivo e quindi facendo clic su **Tutte le azioni → Esegui manualmente Call Home**.Se Centro assistenza clienti Lenovo richiede dati aggiuntivi,

Supporto Lenovo potrebbe richiedere di raccogliere nuovamente i dati di servizio per il dispositivo specifico o per un altro dispositivo.

Per ulteriori informazioni, vedere Apertura di un ticket di assistenza nella documentazione online di XClarity Administrator.

- Riabilitare Call Home in tutti i dispositivi gestiti facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro e quindi su **Tutte le azioni → Abilita Call Home su tutti i dispositivi**.

  Quando si abilita un server d'inoltro di servizio Call Home in Lenovo XClarity Administrator, Call Home è disabilitata in ogni dispositivo gestito, al fine di evitare la creazione di record dei problemi duplicati. Se non si intende più utilizzare XClarity Administrator per gestire i dispositivi o si intende disabilitare Call Home in XClarity Administrator, è possibile riabilitare Call Home in tutti i dispositivi gestiti da XClarity Administrator anziché riabilitare Call Home per ogni singolo dispositivo in un secondo momento.

  Per ulteriori informazioni, vedere Riabilitazione di call home su tutti i dispositivi gestiti nella documentazione online di XClarity Administrator.

Configurazione dell'invio di notifiche automatiche dei problemi al fornitore di servizi preferito

È possibile configurare Lenovo XClarity Administrator in modo che i file di diagnostica, relativi a uno specifico gruppo di dispositivi gestiti, vengano inviati automaticamente al fornitore di servizi preferito (incluso il supporto Lenovo mediante Call Home) affinché determinati eventi che richiedono assistenza, ricevuti dai dispositivi gestiti, (ad esempio, un errore di memoria irreversibile) possano essere risolti.

Prima di iniziare

Attenzione: È necessario accettare l'Informativa sulla privacy di Lenovo prima di poter trasferire i dati al supporto Lenovo.

Accertarsi che tutte le porte richieste da XClarity Administrator (incluse le porte richieste per call home) siano disponibili prima di configurare un server d'inoltro di servizio. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.

Accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti dal fornitore di servizi.

Se si sceglie di utilizzare Supporto Lenovo, accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti da Call Home. Per informazioni sui firewall, vedere Firewall e server proxy nella documentazione online di XClarity Administrator.

Se XClarity Administrator accede a Internet con un proxy HTTP, accertarsi che il server proxy sia configurato come proxy non ricevitore. Per ulteriori informazioni sulla configurazione del proxy, vedere Configurazione dell'accesso alla reteConfigurazione dell'accesso alla rete nella documentazione online di XClarity Administrator.

Informazioni su questa attività

Un *server d'inoltro di servizio* definisce le informazioni sulla destinazione dell'invio dei file di dati di servizio quando si verifica un evento che richiede assistenza. È possibile definire fino a 50 server d'inoltro di servizio.

Per ogni server d'inoltro di servizio, è possibile scegliere di trasferire automaticamente i dati di servizio al supporto Lenovo (denominato *Call Home*), alla funzione Caricamento Lenovo oppure a un altro fornitore di servizi mediante SFTP. Per informazioni sulla configurazione di un server d'inoltro di servizio per Call Home, vedere Configurazione dell'invio di notifiche automatiche dei problemi al Supporto Lenovo (Call Home) e Configurazione dell'invio di notifiche automatiche dei problemi al fornitore di servizi preferito. Per

informazioni sulla configurazione di un server d'inoltro di servizio per la funzione Caricamento Lenovo, vedere Configurazione dell'invio di notifiche automatiche dei problemi alla Funzione Caricamento Lenovo nella documentazione online di XClarity Administrator.

Se un server d'inoltro di servizio è configurato e abilitato per SFTP, XClarity Administrator *trasferisce automaticamente* i dati di servizio raccolti e trasferisce i file di servizio al sito SFTP specificato per il fornitore di servizi preferito.

Per i server con XCC2, XClarity Administrator salva i dati di servizio in due file nel repository.

- **File di servizio**. (.zip) Questo file contiene informazioni su servizio e inventario in un formato facilmente leggibile. Questo file viene inviato automaticamente al fornitore di servizi preferito quando si verifica un evento di manutenzione.
- **File di debug**. (.tzz) Il file contiene tutte le informazioni sul servizio, l'inventario e i log di debug per l'utilizzo da parte del supporto Lenovo. È possibile inviare manualmente questo file al supporto Lenovo, se sono necessarie ulteriori informazioni per risolvere un problema.

Per altri dispositivi, XClarity Administrator salva i dati di servizio (tra cui informazioni su servizio, inventario e log di debug) in un singolo file di servizio nel repository. Questo file viene inviato al fornitore di servizi preferito quando si verifica un evento di manutenzione.

Nota: Se per lo stesso dispositivo sono configurati più server d'inoltro di servizio SFTP, uno solo di essi trasferisce i dati di servizio. L'indirizzo e la porta utilizzati variano a seconda del server d'inoltro di servizio attivato per primo.

Procedura

Per definire e abilitare un server d'inoltro di servizio, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.

Passo 2. Fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro per visualizzare la pagina Server d'inoltro di servizio.

Passo 3. Fare clic sull'icona **Crea server d'inoltro di servizio** ( ) per visualizzare la finestra di dialogo Nuovo server d'inoltro di servizio.

Passo 4. Fare clic sulla scheda **Generale**.

1. Selezionare **SFTP** per il server d'inoltro di servizio:
2. Immettere il nome del server d'inoltro di servizio e una descrizione.

3. Specificare il numero di tentativi di notifica automatici. Il valore predefinito è 2.
4. Specificare il numero minimo di minuti tra i tentativi. Il valore predefinito è 2.
5. (Facoltativo) Fare clic su **Ispezione dati di servizio necessaria** se si desidera controllare i file di servizio prima che vengano trasferiti e, facoltativamente, specificare l'indirizzo e-mail del contatto a cui inviare una notifica quando sarà necessario controllare i file di servizio.

Passo 5. Fare clic sulla scheda **Specifico** e compilare le seguenti informazioni:
- Indirizzo IP e numero di porta del server SFTP
- ID utente e password per l'autenticazione al server SFTP

Passo 6. Fare clic sulla scheda **Dispositivo** e selezionare i dispositivi gestiti e i gruppi di risorse per i quali si desidera che il server d'inoltro di servizio inoltri i dati di servizio.

Suggerimento: per inoltrare dati di servizio per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i dispositivi**.

Passo 7. Fare clic su **Crea**. Il server d'inoltro di servizio viene aggiunto alla pagina Assistenza e supporto

Passo 8. Nella pagina Assistenza e supporto selezionare **Abilita** nella colonna **Stato** per abilitare il server d'inoltro di servizio.

Passo 9. Per evitare che gli eventi che richiedono assistenza nell'elenco degli eventi esclusi aprano automaticamente report dei problemi, selezionare **No** accanto alla domanda **Si desidera che gli eventi esclusi siano in grado di aprire i report dei problemi?**

Passo 10. Selezionare il server d'inoltro di servizio e fare clic su **Test server d'inoltro di servizio** per generare un evento di test per il server d'inoltro di servizio e verificare che XClarity Administrator sia in grado di comunicare con ciascun fornitore.

Nota: Per poter essere testato, il server d'inoltro di servizio deve essere abilitato.

Al termine

Dalla pagina Assistenza e supporto è inoltre possibile procedere come segue:

- Se l'opzione **Ispezione dati di servizio necessaria** è selezionata ed è stato ricevuto un evento che richiede assistenza da uno dei dispositivi gestiti associati al server d'inoltro di servizio, è necessario controllare i file di servizio prima che vengano inoltrati al fornitore di servizi. Per ulteriori informazioni, vedere Analisi dei file di diagnostica nella documentazione online di XClarity Administrator.
- Per modificare le informazioni d'inoltro di servizio, fare clic su **Server d'inoltro di servizio** nel riquadro di navigazione sinistro e fare clic sull'icona **Modifica server d'inoltro di servizio** ( ).
- Per abilitare o disabilitare un fornitore di servizi, fare clic su **Server d'inoltro di servizio** e selezionare **Abilita** o **Disabilita** nella colonna **Stato**.
- Per eliminare il fornitore di servizi, fare clic su **Server d'inoltro di servizio** e selezionare l'icona **Elimina server d'inoltro di servizio** ( ).
- Definire le informazioni di contatto e posizione di supporto per uno specifico dispositivo gestito facendo clic su **Azioni endpoint** nel riquadro di navigazione sinistro, selezionando il dispositivo e quindi facendo clic sull'icona **Crea profilo di contatto** ( ) o sull'icona **Modifica profilo contatto** ( ). Le informazioni di contatto e posizione per il dispositivo gestito sono incluse nel record del problema creato da call home in Centro assistenza clienti Lenovo. Se vengono specificate informazioni di contatto e posizione univoche per un dispositivo gestito, verranno incluse nel record del problema. In caso contrario, verranno utilizzate informazioni generiche specificate per la configurazione call home di XClarity Administrator (nella pagina **Configurazione Call Home** o **Server d'inoltro di servizio**). Per ulteriori informazioni, vedere Definizione dei contatti di supporto per un dispositivo nella documentazione online di XClarity Administrator.
- Raccogliere i dati di servizio per uno specifico dispositivo facendo clic su **Azioni endpoint**, selezionando il dispositivo e quindi facendo clic sull'icona **Raccogli dati di servizio** ( ). Per ulteriori informazioni,

vedere Raccolta e download dei file di diagnostica per un dispositivo nella documentazione online di XClarity Administrator.

Per ulteriori informazioni su queste attività di assistenza e supporto, vedere Utilizzo di assistenza e supporto nella documentazione online di XClarity Administrator.

Connessione di XClarity Administrator come hub al portale TruScale

È possibile connettere Lenovo XClarity Administrator come hub di gestione al portale Lenovo TruScale.

Prima di iniziare

Attenzione: Queste operazioni di configurazione sono destinate solo ai tecnici dell'assistenza Lenovo.

Procedura

Per connettere XClarity Administrator al portale TruScale, completare le operazioni che seguono.

Passo 1. Sulla barra dei menu di XClarity Administrator fare clic su **Amministrazione → Configurazione hub** per visualizzare la pagina Configurazione hub.

Passo 2. Creare una chiave di registrazione facendo clic su **Genera richiesta di registrazione**. Viene visualizzata la finestra di dialogo Genera richiesta di registrazione.

Passo 3. Fare clic su **Copia negli Appunti** per copiare la chiave di registrazione e chiudere la finestra di dialogo.

Passo 4. Fare clic su **Installa chiave di registrazione** per visualizzare la finestra di dialogo Installa chiave di registrazione.

Passo 5. Incollare la chiave di registrazione nel campo **Chiave di registrazione**.

Passo 6. Fare clic su **Invia**.

Al termine

È possibile disinstallare la chiave di registrazione facendo clic su **Reimposta configurazione**.

Backup, ripristino e migrazione delle impostazioni e dei dati di sistema

È possibile utilizzare Lenovo XClarity Administrator per eseguire il backup e il ripristino delle impostazioni e dei dati di sistema, nonché dei file importati, come le immagini del sistema operativo, gli aggiornamenti firmware e i driver di dispositivo del sistema operativo.

Backup di Lenovo XClarity Administrator

Se sono già state implementate procedure di backup per gli host virtuali, assicurarsi che tali procedure includano Lenovo XClarity Administrator.

Prima di iniziare

Attenzione: Accertarsi che tutti gli utenti attivi siano stati avvisati prima di iniziare la procedura di backup. XClarity Administrator rimarrà inattivo durante la procedura per prevenire la modifica dei dati. Pertanto, non è possibile accedere a XClarity Administrator mentre è in esecuzione la procedura di backup.

Verificare che il certificato dell'autorità di certificazione sia stato scaricato dall'appliance virtuale XClarity Administrator e importato nel browser Web (vedere Importazione del certificato dell'Autorità di certificazione in un browser Web).

Verificare che tutti i processi in esecuzione siano stati completati e che non vi siano processi in sospeso. Se i processi sono in esecuzione, è possibile scegliere di interromperli e continuare la creazione del backup.

Accertarsi che i server DNS siano configurati correttamente; in caso contrario, SMTP e NTP potrebbero non funzionare correttamente una volta ripristinato il backup.

Verificare che sul disco del server di gestione sia disponibile spazio sufficiente per il backup. In caso contrario, liberare spazio su disco eliminando le risorse di XClarity Administrator, come i backup precedenti, che non sono più necessarie (vedere Gestione dello spazio su disco) oppure creare un nuovo backup senza includere le immagini del sistema operativo, gli aggiornamenti firmware e i driver di dispositivo del sistema operativo.

Accertarsi che la distribuzione del sistema operativo sia configurata sull'interfaccia di rete appropriata, eth1 o eth0, se si desidera eseguire il backup delle immagini del sistema operativo (vedere Configurazione dell'accesso alla rete).

Informazioni su questa attività

Eseguire sempre il backup di XClarity Administrator dopo aver eseguito la configurazione iniziale e dopo aver apportato modifiche significative alla configurazione, incluse le situazioni seguenti:

- Prima di eseguire l'aggiornamento di XClarity Administrator
- Quando si gestiscono nuovi chassis o server rack
- Quando si aggiungono utenti a XClarity Administrator
- Quando si creano e distribuiscono nuovi pattern di configurazione

Assicurarsi di eseguire backup regolari di XClarity Administrator.

Si consiglia di scaricare i backup nel sistema locale. Se il sistema operativo host si arresta in modo imprevisto, non è possibile eseguire l'autenticazione con XClarity Administrator dopo che tale sistema operativo host sarà stato riavviato. Per risolvere questo problema, ripristinare l'ultimo backup di XClarity Administrator sul sistema locale (vedere Ripristino di Lenovo XClarity Administrator.).

Procedura

Per eseguire il backup di XClarity Administrator, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Backup e ripristino dei dati**. Verrà visualizzata la pagina "Backup e ripristino dei dati".

Passo 2. Fare clic sull'icona **Backup** (). Verrà visualizzata la pagina Dati di backup e impostazioni.

Passo 3. Immettere una descrizione per il backup.

Passo 4. Scegliere la posizione in cui si desidera creare il backup. Il backup può essere creato nel repository locale o su una condivisione remota.

Per impostazione predefinita, il backup viene creato nel repository locale. È possibile copiare un backup dal repository locale a una condivisione remota facendo clic sull'icona **Copia backup** ().

Se si sceglie una condivisione remota, il backup viene creato prima nel repository locale. Quindi, il backup viene copiato nella condivisione remota selezionata e la copia locale viene eliminata. Per ulteriori informazioni, vedere Gestione condivisioni remote.

Passo 5. Facoltativamente, scegliere di includere le immagini del sistema operativo, gli aggiornamenti firmware e i driver di dispositivo del sistema operativo.

Passo 6. Specificare la passphrase di crittografia per il backup.

Attenzione: Registrare la passphrase di crittografia. La passphrase è necessaria per ripristinare il backup per questa o un'altra istanza di XClarity Administrator. Se si dimentica la passphrase, non vi è alcun modo per recuperala.

Passo 7. Fare clic su **Backup** per eseguire subito il backup di dati e impostazioni oppure fare clic su **Pianifica** per pianificare l'esecuzione di questo backup in un secondo momento.

Attenzione: Se si sceglie di eseguire il backup immediatamente, non chiudere o aggiornare la scheda del browser Web o la finestra prima che il processo venga completato. In caso contrario, potrebbe non essere possibile generare il backup.

La creazione del backup potrebbe richiedere tempo. Viene visualizzata una barra di avanzamento dello stato del processo.

Se si sceglie di creare il backup su una condivisione remota, è possibile monitorarne l'avanzamento dalla pagina Processi (vedere Monitoraggio dei processi).

Se si pianifica un backup, il server di gestione viene arrestato temporaneamente durante il processo di backup. Una volta ripristinato il server di gestione, è possibile monitorare lo stato del processo di backup dalla pagina Processi.

Passo 8. Eseguire il login a XClarity Administrator per continuare a gestire i dispositivi.

Al termine

Dalla pagina "Backup e ripristino dei dati" è possibile eseguire le seguenti azioni:

- Copiare i backup di XClarity Administrator da o verso una condivisione remota facendo clic sull'icona **Copia backup** ( ).
- Eliminare i backup selezionati non più necessari dal repository locale o dalle condivisioni remote, facendo clic sull'icona **Elimina backup** ( ).
- Ripristinare le impostazioni e i dati di sistema in questo server di gestione (vedere Ripristino di Lenovo XClarity Administrator).
- Importare o esportare i backup dal sistema locale, facendo clic rispettivamente sull'icona **Importa backup** ( ) o **Esporta backup** ( ).
- Eseguire il push del backup selezionato su una nuova istanza di XClarity Administrator (vedere Migrazione dei dati di sistema e delle impostazioni su un'altra istanza di XClarity Administrator).

Ripristino di Lenovo XClarity Administrator

È possibile utilizzare il backup dei dati e delle impostazioni per ripristinare Lenovo XClarity Administrator a uno stato precedente.

Prima di iniziare

Attenzione: Accertarsi che tutti gli utenti attivi siano stati avvisati prima di iniziare la procedura di backup. XClarity Administrator rimarrà inattivo durante la procedura per prevenire la modifica dei dati. Pertanto, non è possibile accedere a XClarity Administrator mentre è in esecuzione la procedura di backup

Scaricare il certificato dell'autorità di certificazione dall'appliance virtuale XClarity Administrator e importarlo nel browser Web (vedere Importazione del certificato dell'Autorità di certificazione in un browser Web).

Verificare che tutti i processi in esecuzione siano stati completati e che non vi siano processi in sospeso.

È possibile ripristinare un backup solo per la stessa versione di XClarity Administrator utilizzata per creare il backup.

Informazioni su questa attività

Attenzione:

- Tutte le modifiche apportate dopo la creazione del backup andranno perse.
- Per ripristinare i dati, l'appliance virtuale viene reimpostata allo stato originario. Prima di ripristinare i dati del backup, tutte le impostazioni correnti, l'inventario del dispositivo e i file (le immagini del sistema operativo, gli aggiornamenti firmware e i driver di dispositivo del sistema operativo) vengono eliminati. I dati e le impostazioni del backup non vengono uniti alle impostazioni e ai dati correnti dell'appliance virtuale. Se si sceglie di non ripristinare l'inventario del dispositivo, le immagini del sistema operativo, gli aggiornamenti firmware e i driver di dispositivo del sistema operativo, solo i dati XClarity Administrator predefiniti sono presenti al termine dell'operazione di ripristino.

Il ripristino di un backup non elimina i backup dell'istanza XClarity Administrator.

Il ripristino di un backup non modifica i dati o le impostazioni dei dispositivi gestiti. Ad esempio, se si annulla la gestione di un dispositivo e quindi si ripristina un backup precedente quando il dispositivo è ancora gestito su XClarity Administrator, potrebbe verificarsi problemi di connettività del dispositivo al termine dell'operazione di ripristino. Analogamente, se si gestisce un dispositivo e quindi si ripristina un backup precedente quando il dispositivo non è ancora gestito, potrebbe essere necessario modificare manualmente la configurazione del dispositivo per annullare lo stato gestito o utilizzare l'opzione **Forza** quando si tenta di gestirlo nuovamente in XClarity Administrator.

Procedura

Completare le seguenti operazioni per ripristinare XClarity Administrator.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Backup e ripristino dei dati**. Verrà visualizzata la pagina "Backup e ripristino dei dati".

Passo 2. Se si esporta il pacchetto di backup nel sistema locale e lo si elimina da XClarity Administrator, completare le seguenti operazioni.

a. Dalla pagina "Backup e ripristino dei dati", fare clic sull'icona **Importa backup** () per visualizzare la finestra di dialogo "Importa backup".

b. Fare clic su **Sfoglia** per individuare il backup esportato da un'istanza XClarity Administrator.

c. Fare clic su **Importa** per caricare il backup in XClarity Administrator.

L'importazione del backup potrebbe richiedere tempo. Viene visualizzata una barra di avanzamento dello stato del processo.

Attenzione: Se si chiude o si aggiorna la finestra o la scheda del browser Web prima che il caricamento venga completato, potrebbe non essere possibile completare il processo.

d. Una volta completata l'importazione, specificare la passphrase di crittografia per il backup.

Nota: Se non si dispone della passphrase di crittografia, è necessario creare un nuovo backup in XClarity Administrator (vedere Backup di Lenovo XClarity Administrator).

Passo 3. Selezionare il backup da ripristinare e fare clic sull'icona **Ripristina backup** (). Viene visualizzata la finestra di dialogo Ripristino dei dati.

Passo 4. Specificare la passphrase di crittografia per il backup.

Passo 5. Fare clic su **Conferma**.

Passo 6. Nella finestra di dialogo "Conferma ripristino dati", verificare che le informazioni siano corrette.

Passo 7. Nella finestra di dialogo "Opzioni di ripristino" scegliere facoltativamente di importare le immagini del sistema operativo, gli aggiornamenti firmware, i driver di dispositivo del sistema operativo, le impostazioni di rete e l'inventario dei dispositivi.

Attenzione: Leggere attentamente le avvertenze visualizzate in questa finestra di dialogo.

Passo 8. Fare clic su **Conferma** per avviare il ripristino dei dati.

Il ripristino dei dati e delle impostazioni potrebbe richiedere tempo. Viene visualizzata una barra di avanzamento dello stato del processo.

Una volta completato il processo di ripristino, si verrà reindirizzati alla pagina di login.

Attenzione: Se si chiude o si aggiorna la finestra o la scheda del browser Web prima che il processo venga completato, potrebbe non essere possibile completare l'operazione.

Passo 9. Eseguire il login a XClarity Administrator per continuare a gestire i dispositivi.

Migrazione dei dati di sistema e delle impostazioni su un'altra istanza di XClarity Administrator

È possibile eseguire la migrazione delle impostazioni e dei dati del sistema di cui è stato creato il backup, su una nuova istanza di Lenovo XClarity Administrator che si trova nella stessa rete o in un'altra rete.

Prima di iniziare

Il server di gestione di destinazione deve essere una *nuova* istanza di XClarity Administrator con la stessa versione del server di gestione usata per creare il backup e deve trovarsi nella prima fase (nessun passaggio completato) della procedura guidata Configurazione iniziale. Per ulteriori informazioni, vedere Installazione e configurazione di XClarity Administrator nella documentazione online di XClarity Administrator.

Accertarsi che tutti gli utenti attivi siano stati avvisati prima di iniziare la procedura di backup. XClarity Administrator rimarrà inattivo durante la procedura per prevenire la modifica dei dati. Pertanto, non è possibile accedere a XClarity Administrator mentre è in esecuzione la procedura di backup.

Scaricare il certificato dell'autorità di certificazione dall'appliance virtuale XClarity Administrator e importarlo nel browser Web (vedere Gestione dello spazio su disco nella documentazione online di XClarity Administrator).

Non viene eseguita la migrazione sul server di gestione di destinazione dei backup che si trovano nel repository dei backup del server di gestione di origine. Prima di eseguire la migrazione dei dati e delle impostazioni, esportare i backup che potrebbero essere necessari nel sistema locale.

Informazioni su questa attività

Non verrà eseguita la migrazione sul server di gestione di destinazione di eventuali modifiche al server di gestione di origine successive alla creazione del backup.

Il ripristino di un backup non modifica i dati o le impostazioni dei dispositivi gestiti. Ad esempio, se si annulla la gestione di un dispositivo e quindi si ripristina un backup precedente quando il dispositivo è ancora gestito su XClarity Administrator, potrebbe verificarsi problemi di connettività del dispositivo al termine dell'operazione di ripristino. Analogamente, se si gestisce un dispositivo e quindi si ripristina un backup precedente quando il dispositivo non è ancora gestito, potrebbe essere necessario modificare manualmente la configurazione del dispositivo per annullare lo stato gestito o utilizzare l'opzione **Forza** quando si tenta di gestirlo nuovamente in XClarity Administrator.

Nota: Quando si esegue XClarity Administrator come un contenitore, i volumi creati nell'host per un contenitore possono essere utilizzati come volumi da un altro contenitore. Una volta associati i volumi al nuovo contenitore (destinazione), non possono più essere utilizzati dal contenitore iniziale (origine).

1. Configurazione del file `docker-componee.yml` per il contenitore di destinazione in modo da utilizzare lo stesso indirizzo IP e il nome del contenitore come contenitore di origine.
2. Interrompere il contenitore di origine utilizzando il comando seguente.
   `docker-compose -p ${CONTAINER_NAME} down`
3. Avviare il contenitore di destinazione utilizzando il comando seguente, dove <*env_filename*> è il nome del file delle variabili di ambiente. All'avvio del contenitore di destinazione, i volumi vengono associati al contenitore di destinazione XClarity Administrator e XClarity Administrator utilizza i dati e le impostazioni di sistema di questi volumi.
   COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d`

Procedura

Completare le seguenti operazioni per ripristinare XClarity Administrator.

Passo 1. Se i sistemi XClarity Administrator di origine e destinazione si trovano nella stessa rete, completare le seguenti operazioni.

a. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Backup e ripristino dei dati**. Verrà visualizzata la pagina "Backup e ripristino dei dati".

b. Fare clic sull'icona **Push Backup** ( ) per visualizzare la finestra di dialogo "Push dei dati".

c. Specificare l'indirizzo IP corrente del sistema XClarity Administrator di destinazione.

d. Fare clic su **Continua** per caricare il backup sul sistema XClarity Administrator di destinazione.

   Il caricamento del backup potrebbe richiedere tempo. Viene visualizzata una barra di avanzamento dello stato del processo.

   Attenzione: Se si chiude o si aggiorna la finestra o la scheda del browser Web prima che il caricamento venga completato, potrebbe non essere possibile caricare il pacchetto.

Passo 2. Se i sistemi XClarity Administrator di origine e destinazione *non* si trovano nella stessa rete, completare le seguenti operazioni.

a. Dalla barra dei menu del sistema XClarity Administrator di origine, fare clic su **Amministrazione → Backup e ripristino dei dati**. Dalla pagina "Backup e ripristino dei dati", fare clic sull'icona **Esporta backup** icona ( ) per esportare il backup nel sistema locale.

   L'esportazione del backup potrebbe richiedere tempo.

b. Copiare il backup esportato dal server di gestione di origine su un sistema nella stessa rete del server di gestione di destinazione

c. Dalla pagina della procedura guidata del sistema XClarity Administrator di destinazione, fare clic sull'icona **Importa backup** ( ) per visualizzare la finestra di dialogo "Importa pacchetto di dati".

d. Fare clic su **Sfoglia** per individuare il backup esportato dal sistema XClarity Administrator di origine.

e. Fare clic su **Carica** per importare il backup sul sistema XClarity Administrator di destinazione.

   L'importazione del backup potrebbe richiedere tempo. Viene visualizzata una barra di avanzamento dello stato del processo.

Attenzione: Se si chiude o si aggiorna la finestra o la scheda del browser Web prima che il caricamento venga completato, potrebbe non essere possibile completare il processo.

Passo 3. Una volta completata l'importazione, specificare la passphrase di crittografia per il backup.

Nota: Se non si dispone della passphrase di crittografia, è necessario creare un nuovo backup sul sistema XClarity Administrator di origine (vedere Backup di Lenovo XClarity Administrator.

Passo 4. Nella finestra di dialogo "Conferma ripristino dati", verificare che tutte le informazioni siano corrette.

Passo 5. Fare clic su **Conferma** per avviare il caricamento delle impostazioni e dei dati di sistema.

Passo 6. Nella finestra di dialogo "Opzioni di ripristino" scegliere facoltativamente di importare le immagini del sistema operativo, gli aggiornamenti firmware, i driver di dispositivo del sistema operativo, le impostazioni di rete e l'inventario dei dispositivi.

Attenzione: Leggere attentamente le avvertenze visualizzate in questa finestra di dialogo.

Passo 7. Se si sceglie di importare le impostazioni di rete o l'inventario di un dispositivo, arrestare il server di gestione di origine dal sistema XClarity Administrator di origine, facendo clic su **Amministrazione → Arresta il server di gestione → Arresta**.

Verificare che l'appliance virtuale di origine sia stata arrestata prima di continuare

Passo 8. Sul sistema XClarity Administrator di destinazione, fare clic su **Conferma** per avviare il caricamento dei dati e delle impostazioni dal pacchetto

Se si sceglie di importare le impostazioni di rete, al termine della migrazione gli indirizzi IP del sistema XClarity Administrator di origine vengono riassegnati al sistema XClarity Administrator di destinazione.

Attenzione: Se il sistema XClarity Administrator di origine utilizza il protocollo DHCP, è necessario associare gli indirizzi MAC del sistema XClarity Administrator di destinazione agli indirizzi IP del sistema XClarity Administrator di origine corrispondente, sul server DHCP. Prima di continuare, attendere almeno 15 minuti dopo la modifica del server DHCP.

Passo 9. Attendere il completamento della barra di avanzamento "Caricamento dati e impostazioni dal pacchetto".

Una volta completato il processo di migrazione dei dati, si verrà reindirizzati alla pagina di login.

Attenzione: Se si chiude o si aggiorna la finestra o la scheda del browser Web prima che il caricamento venga completato, potrebbe non essere possibile completare il processo.

Passo 10. Eseguire il login al sistema XClarity Administrator di destinazione per continuare a gestire i dispositivi.

Gestione dello spazio su disco

È possibile gestire la quantità di spazio su disco utilizzato da Lenovo XClarity Administrator, spostando i file di dati di grandi dimensioni non immediatamente necessari in una condivisione remota. In alternativa, è possibile eliminare le risorse non più necessarie.

Informazioni su questa attività

Per determinare lo spazio su disco attualmente utilizzato, fare clic su **Dashboard** dalla barra di menu di XClarity Administrator. L'utilizzo dello spazio sul disco del repository e delle condivisioni remote è riportato nella sezione Attività di XClarity Administrator.

Procedura

Completare una o più delle seguenti operazioni per liberare lo spazio su disco spostando i file su una condivisione remota ed eliminando le risorse non necessarie.

- **Eliminazione delle risorse non necessarie**

  È possibile eliminare rapidamente dal repository locale i file che non sono più necessari completando le seguenti operazioni.

  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Pulizia disco** per visualizzare la pagina Pulizia disco.
  2. Selezionare i file che si desidera eliminare. L'intestazione della sezione identifica la quantità di spazio che verrà liberata quando i file verranno eliminati.
     - **File correlati al sistema operativo**

       È possibile eliminare le immagini del sistema operativo, i file con opzioni di avvio e i file di software.
     - **Aggiornamenti firmware**

       È possibile eliminare i file di payload per tutti i driver di dispositivo del sistema operativo associati a UpdateXpress System Packs (UXSPs) e singoli driver di dispositivo con stato Scaricato.

       È possibile eliminare i file di payload per i singoli aggiornamenti firmware con stato Scaricato non utilizzati da un criterio di conformità del firmware.

       È possibile eliminare i file di payload del server di gestione con stato Scaricato.

       Nota: Quando il repository degli aggiornamenti firmware si trova in una condivisione remota, non è possibile utilizzare la funzione di pulizia del disco per eliminare i singoli aggiornamenti firmware e gli UXSP.
     - **File dei dati di servizio**

       Quando si verifica un evento di servizio su un dispositivo, i dati di servizio vengono raccolti automaticamente per tale dispositivo. I dati di servizio vengono automaticamente acquisiti per il server di gestione ogni volta che si verifica un'eccezione in XClarity Administrator. Si consiglia di eliminare periodicamente questi archivi se XClarity Administrator e i dispositivi gestiti sono in esecuzione senza problemi.

       Quando gli aggiornamenti del server di gestione vengono applicati correttamente, i file di aggiornamento vengono eliminati automaticamente dal repository.
  3. Fare clic su **Elimina elementi selezionati**.
  4. Esaminare l'elenco dei file selezionati e fare clic su **Elimina**.
- **Spostare i pacchetti di aggiornamento firmware in un repository remoto**

  Per impostazione predefinita, Lenovo XClarity Administrator utilizza un repository (interno) locale per gli aggiornamenti firmware disponibili. È possibile liberare lo spazio su disco disponibile nel repository locale XClarity Administrator utilizzando una condivisione remota montata su SSH File System (SSHTF) come repository remoto. È quindi possibile utilizzare i file di aggiornamento firmware direttamente dal repository remoto per mantenere la conformità del firmware sui dispositivi. Per ulteriori informazioni, vedere Utilizzo di un repository remoto per gli aggiornamenti firmware.

  Quando si modifica la posizione del repository degli aggiornamenti firmware, è possibile scegliere di copiare tutti gli aggiornamenti firmware dal repository originale al nuovo repository.

  I file di aggiornamento firmware nel repository originale *non vengono* puliti automaticamente dopo il cambio di posizione.

Suggerimento: il repository degli aggiornamenti remoti può essere condiviso da più server di gestione XClarity Administrator.

Per spostare gli aggiornamenti firmware in un repository degli aggiornamenti firmware remoto, completare le seguenti operazioni.

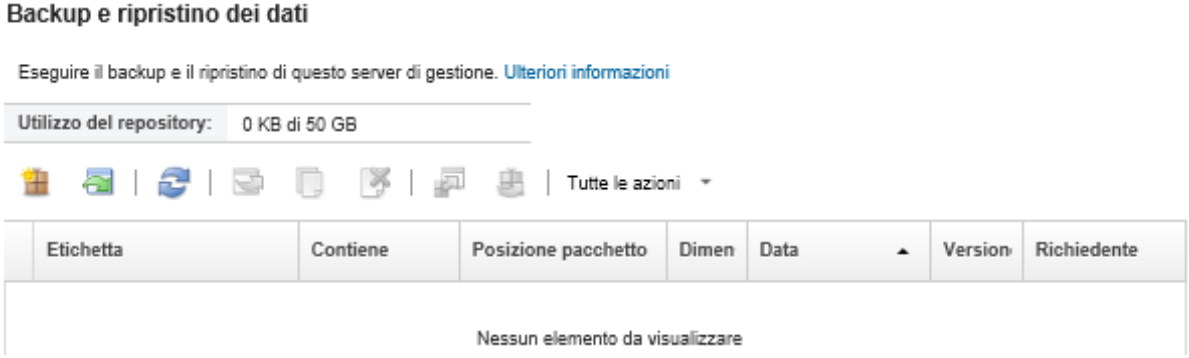
1. Aggiungere una condivisione remota a XClarity Administrator (vedere Gestione condivisioni remote).
2. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Repository**. Viene visualizzata la pagina Repository aggiornamenti firmware.
3. Fare clic su **Tutte le azioni → Posizione repository switch** per visualizzare la finestra di dialogo Posizione repository switch.
4. Selezionare la condivisione remota appena creata dall'elenco a discesa **Posizione repository**.
5. Selezionare **Copia pacchetti di aggiornamento dal repository corrente nel nuovo repository** per copiare i file di aggiornamento firmware nella nuova posizione del repository prima di passare alla posizione del repository.
6. Fare clic su **OK**.

   Viene creato un processo per copiare i pacchetti di aggiornamento firmware nel nuovo repository. Per monitorare l'avanzamento del processo, fare clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator.
7. Pulire i file di aggiornamento firmware nel repository locale.
   a. Passare al repository locale facendo clic su **Tutte le azioni → Posizione repository switch**, selezionare **Repository locale** per la posizione del repository, quindi fare clic su **OK**.
   b. Fare clic sulla scheda **Aggiornamenti individuali**, selezionare la casella di controllo Seleziona tutto nella tabella per selezionare tutti gli aggiornamenti firmware, quindi fare clic sull'icona **Elimina pacchetti di aggiornamento completi** ()
   c. Fare clic sulla scheda **UpdateXpress System Pack (UXSP)**, selezionare la casella di controllo Seleziona tutto nella tabella per selezionare tutti gli UXSP, quindi fare clic sull'icona **Elimina UXSP e criterio associato** ()
   d. Tornare al repository remoto locale facendo clic su **Tutte le azioni → Posizione repository switch**, selezionare il nuovo repository remoto per la posizione del repository, quindi fare clic su **OK**.

- **Spostamento dei backup di XClarity Administrator in una condivisione remota**

  È possibile liberare spazio sul disco disponibile per il repository locale di XClarity Administrator spostando i backup di XClarity Administrator in una condivisione remota. Tuttavia, non è possibile utilizzare i file direttamente sulla condivisione remota. Per utilizzare i file, è necessario riportarli nel repository locale XClarity Administrator. Per ulteriori informazioni su condivisioni remote, vedere Gestione condivisioni remote.

  Importante: Si consiglia di scaricare i backup sul sistema locale o di copiare i backup in una condivisione remota prima di eliminare i backup in XClarity Administrator.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Backup e ripristino dei dati** per visualizzare la pagina Backup e ripristino dei dati.


   La colonna **Posizione pacchetto** indica se il backup è memorizzato in locale nel repository locale di XClarity Administrator o su una condivisione remota.

2. Selezionare il backup e fare clic sull'icona **Copia backup** ( ) per visualizzare la finestra di dialogo Copia backup.
3. Scegliere la condivisione remota per archiviare il backup.
4. Fare clic su **Copia**.
5. Monitorare l'avanzamento della copia nella pagina Processi. Una volta completata la copia, selezionare nuovamente il backup e fare clic sull'icona **Elimina backup** ( ) per visualizzare finestra di dialogo Elimina backup.
6. Selezionare "Locale" per la posizione.
7. Fare clic su **Elimina**.

Gestione condivisioni remote

È possibile montare condivisioni remote e quindi spostare file di dati di grandi dimensioni, come backup e aggiornamenti firmware di Lenovo XClarity Administrator dal repository locale alla condivisione remota per gestire lo spazio su disco disponibile per il server di gestione.

Prima di iniziare

Quando viene eseguito XClarity Administrator come contenitore, le condivisioni remote vengono montate nel contenitore utilizzando il file yml durante l'installazione (vedere Installazione di XClarity Administrator in ambienti basati su VMware ESXi nella documentazione online di XClarity Administrator).

Quando viene eseguito XClarity Administrator come appliance virtuale, è necessario disporre dell'autorità **lxc-supervisor** per montare o smontare una condivisione remota.

Verificare che sia disponibile una connessione di rete ad alta velocità e stabile tra il file server e XClarity Administrator.

Le connessioni remote non sono supportate quando XClarity Administrator viene eseguito come contenitore.

Informazioni su questa attività

È necessario utilizzare condivisioni remote separate per memorizzare i backup e gli aggiornamenti firmware di XClarity Administrator.

Non è possibile utilizzare i file di backup di XClarity Administrator direttamente dalla condivisione remota. Per utilizzare i file di backup, è necessario riportarli nel repository locale .

Attualmente, è supportato solo SSHFS.

Procedura

Per aggiungere una condivisione remota quando è in esecuzione XClarity Administrator come appliance virtuale, completare la seguente procedura.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Condivisione remota**. Viene visualizzata la pagina Condivisione remota.
2. Fare clic sull'icona **Crea** ( ) per creare una condivisione remota. Viene visualizzata la finestra di dialogo Crea condivisione remota.
3. Specificare l'indirizzo IP del file server che ospita la condivisione remota.
4. Specificare le credenziali memorizzate da utilizzare per accedere alla condivisione remota.

   Suggerimento: per creare una credenziale memorizzata, vedere Gestione delle credenziali memorizzate.
5. Specificare il punto di montaggio (directory locale) sul server di gestione da utilizzare per montare la condivisione remota.

   Importante: Il percorso deve iniziare con "/mnt".
6. Specificare la directory condivisa (percorso del server remoto) da montare come condivisione remota sul server di gestione.
7. Fare clic su **Crea**.

Al termine

- Smontare la condivisione remota selezionandola e facendo clic sull'icona **Elimina** ( ).
- Spostare i file di backup di XClarity Administrator da e verso una condivisione remota (vedere Gestione dello spazio su disco).
- Configurare XClarity Administrator per utilizzare una condivisione remota come repository degli aggiornamenti firmware (vedere Utilizzo di un repository remoto per gli aggiornamenti firmware.

Modifica della lingua dell'interfaccia utente

È possibile modificare la lingua dell'interfaccia utente dopo aver effettuato il login.

Procedura

Nella barra del titolo di Lenovo XClarity Administrator, fare clic sul menu azioni utente (ADMIN_USER) e quindi su **Modifica lingua**. Selezionare la lingua che si desidera visualizzare, quindi fare clic su **Chiudi**.

Nota: Il sistema di guida viene visualizzato nella stessa lingua impostata per l'interfaccia utente.

Arresto di XClarity Administrator

Quando Lenovo XClarity Administrator viene arrestato, si perde la connettività a Lenovo XClarity Administrator.

Prima di iniziare

È necessario disporre dell'autorità **lxc-supervisor** o **lxc-admin** per arrestare l'appliance virtuale XClarity Administrator.

Verificare che non ci siano processi in esecuzione. Tutti i processi attualmente in esecuzione verranno annullati durante il processo di arresto. Per visualizzare il log processi, vedere Monitoraggio dei processi.

Procedura

Completare la procedura riportata di seguito per arrestare Lenovo XClarity Administrator.

- **Contenitori**

  Eseguire i seguenti comandi per arrestare il contenitore.
  ```
  docker-compose -p ${CONTAINER_NAME} down
  ```
- **Appliance virtuali**
  1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Arresta server di gestione**.

     Viene visualizzata una finestra di dialogo di conferma video con un elenco dei processi attualmente in esecuzione. Quando si arresta XClarity Administrator, i processi vengono annullati.
  2. Fare clic su **Arresta**.

Al termine

Per riavviare XClarity Administrator dopo un arresto, vedere Riavvio di XClarity Administrator.

Riavvio di XClarity Administrator

È possibile riavviare Lenovo XClarity Administrator dall'interfaccia Web o dall'hypervisor dopo un arresto.

Prima di iniziare

È necessario disporre dell'autorità **lxc-supervisor** o **lxc-admin** per riavviare XClarity Administrator.

Verificare che non ci siano processi in esecuzione. I processi in esecuzione verranno annullati durante il riavvio. Per visualizzare il log processi, vedere Monitoraggio dei processi.

Informazioni su questa attività

Esistono alcune situazioni in cui viene richiesto di eseguire il riavvio: Lenovo XClarity Administrator
- Quando si rigenera un certificato server
- Quando si carica un nuovo certificato server

Procedura

Completare una delle seguenti procedure per riavviare Lenovo XClarity Administrator.

- **Contenitori**

  Eseguire i comandi seguenti per arrestare e quindi avviare il contenitore, dove <*env_filename*> è il nome del file delle variabili di ambiente.
  ```
  docker-compose -p ${CONTAINER_NAME} down
  COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
  ```
- **Appliance virtuali**

– Riavvio di Lenovo XClarity Administrator dall'interfaccia Web:

1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Arresta server di gestione**.

   Viene visualizzata una finestra di dialogo di conferma video con un elenco dei processi attualmente in esecuzione. Quando si riavvia Lenovo XClarity Administrator, i processi vengono annullati.

2. Fare clic su **Riavvia**.

   Quando Lenovo XClarity Administrator viene arrestato, si perde la connettività a Lenovo XClarity Administrator.

3. Attendere alcuni minuti il riavvio di Lenovo XClarity Administrator, quindi eseguire nuovamente il login.

– Riavvio di Lenovo XClarity Administrator dall'hypervisor dopo un arresto:

  – Microsoft Hyper-V

    1. Dal dashboard Server Manager fare clic su **Hyper-V**.
    2. Fare clic con il pulsante destro del mouse sul server e scegliere **Hyper-V Manager**.
    3. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Avvia**. All'avvio della macchina virtuale, verranno elencati gli indirizzi IPv4 e IPv6 per ogni interfaccia, come riportato nell'esempio seguente.

       Per impostazione predefinita, la porta di gestione eth0 di XClarity Administrator utilizza un indirizzo IP DHCP. Al termine del processo di avvio di XClarity Administrator è possibile configurare un indirizzo IP statico per la porta di gestione eth0, immettendo 1 quando richiesto, come mostrato nel seguente esempio. La richiesta è disponibile per 150 secondi, finché non viene visualizzata la richiesta di login. Per accedere subito alla richiesta di login, immettere x quando richiesto.

       Importante:

       - Quando si modificano le impostazioni degli indirizzi IP statici, sono disponibili massimo 60 secondi per immettere le nuove impostazioni. Prima di continuare, accertarsi di disporre delle informazioni richieste relative agli IP.
         – Per le impostazioni IPv4, è necessario disporre di indirizzo IP, maschera di sottorete e indirizzo IP del gateway
         – Per le impostazioni IPv6, è necessario disporre dell'indirizzo IP e della lunghezza del prefisso
       - Se non si utilizza un server DHCP, è possibile utilizzare un file di configurazione per specificare le impostazioni IP della porta di gestione eth0 di XClarity Administrator che si desidera utilizzare per accedere all'interfaccia Web di XClarity Administrator. Per ulteriori informazioni, vedere la sezione "Operazioni successive", riportata di seguito.
       - Se si modificano le impostazioni degli indirizzi IP dalla console, XClarity Administrator viene riavviato per applicare le nuove impostazioni.
       - Non è richiesta alcuna azione per eseguire il login. Ignorare il messaggio di login alla console. L'interfaccia della console non è destinata all'uso da parte dei clienti.
       - La console potrebbe visualizzare il messaggio `TCP: eth0: l'implementazione GRO del driver è sospetta: le prestazioni TCP potrebbero essere ridotte`. Le prestazioni della macchina virtuale restano invariate ed è possibile ignorare questa avvertenza.

       Attenzione: La modifica dell'indirizzo IP della porta di gestione di XClarity Administrator dopo la gestione dei dispositivi potrebbe determinare l'attivazione dello stato offline dei dispositivi in XClarity Administrator. Se si sceglie di modificare l'indirizzo IP dopo che XClarity Administrator è attivo e in esecuzione, verificare che tutti i dispositivi risultino non gestiti prima di modificare l'indirizzo IP.

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  ... ...
```

4. Eseguire il login a Lenovo XClarity Administrator (vedere Login a XClarity Administrator).

– VMware ESXi

1. Collegarsi all'host mediante VMware vSphere Client.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Alimentazione → Accendi**.
3. Selezionare la scheda **Console**. All'avvio della macchina virtuale, verranno elencati gli indirizzi IPv4 e IPv6 per ogni interfaccia, come riportato nell'esempio seguente.

   Per impostazione predefinita, la porta di gestione eth0 di XClarity Administrator utilizza un indirizzo IP DHCP. Al termine del processo di avvio di XClarity Administrator è possibile configurare un indirizzo IP statico per la porta di gestione eth0, immettendo 1 quando richiesto, come mostrato nel seguente esempio. La richiesta è disponibile per 150 secondi, finché non viene visualizzata la richiesta di login. Per accedere subito alla richiesta di login, immettere x quando richiesto.

   Importante:

   - Quando si modificano le impostazioni degli indirizzi IP statici, sono disponibili massimo 60 secondi per immettere le nuove impostazioni. Prima di continuare, accertarsi di disporre delle informazioni richieste relative agli IP.
     – Per le impostazioni IPv4, è necessario disporre di indirizzo IP, maschera di sottorete e indirizzo IP del gateway
     – Per le impostazioni IPv6, è necessario disporre dell'indirizzo IP e della lunghezza del prefisso
   - Se non si utilizza un server DHCP, è possibile utilizzare un file di configurazione per specificare le impostazioni IP della porta di gestione eth0 di XClarity Administrator che si desidera utilizzare per accedere all'interfaccia Web di XClarity Administrator. Per ulteriori informazioni, vedere la sezione "Operazioni successive", riportata di seguito.
   - Se si modificano le impostazioni degli indirizzi IP dalla console, XClarity Administrator viene riavviato per applicare le nuove impostazioni.
   - Non è richiesta alcuna azione per eseguire il login. Ignorare il messaggio di login alla console. L'interfaccia della console non è destinata all'uso da parte dei clienti.
   - La console potrebbe visualizzare il messaggio `TCP: eth0: l'implementazione GRO del driver è sospetta: le prestazioni TCP potrebbero essere ridotte`. Le prestazioni della macchina virtuale restano invariate ed è possibile ignorare questa avvertenza.

Attenzione: La modifica dell'indirizzo IP della porta di gestione di XClarity Administrator dopo la gestione dei dispositivi potrebbe determinare l'attivazione dello stato offline dei dispositivi in XClarity Administrator. Se si sceglie di modificare l'indirizzo IP dopo che XClarity Administrator è attivo e in esecuzione, verificare che tutti i dispositivi risultino non gestiti prima di modificare l'indirizzo IP.

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  ... ...
```

4. Eseguire il login a Lenovo XClarity Administrator (vedere Login a XClarity Administrator).

Al termine

Quando Lenovo XClarity Administrator viene riavviato, raccoglie nuovamente l'inventario per ogni dispositivo gestito. Attendere circa 30-45 minuti, a seconda del numero di dispositivi gestiti, prima di provare ad eseguire gli aggiornamenti firmware, le distribuzioni dei pattern di configurazione o le distribuzioni del sistema operativo.

Capitolo 3. Monitoraggio di dispositivi e attività

È possibile monitorare i dispositivi e le attività tramite il dashboard, gli avvisi, i log di controllo e i log dei processi.

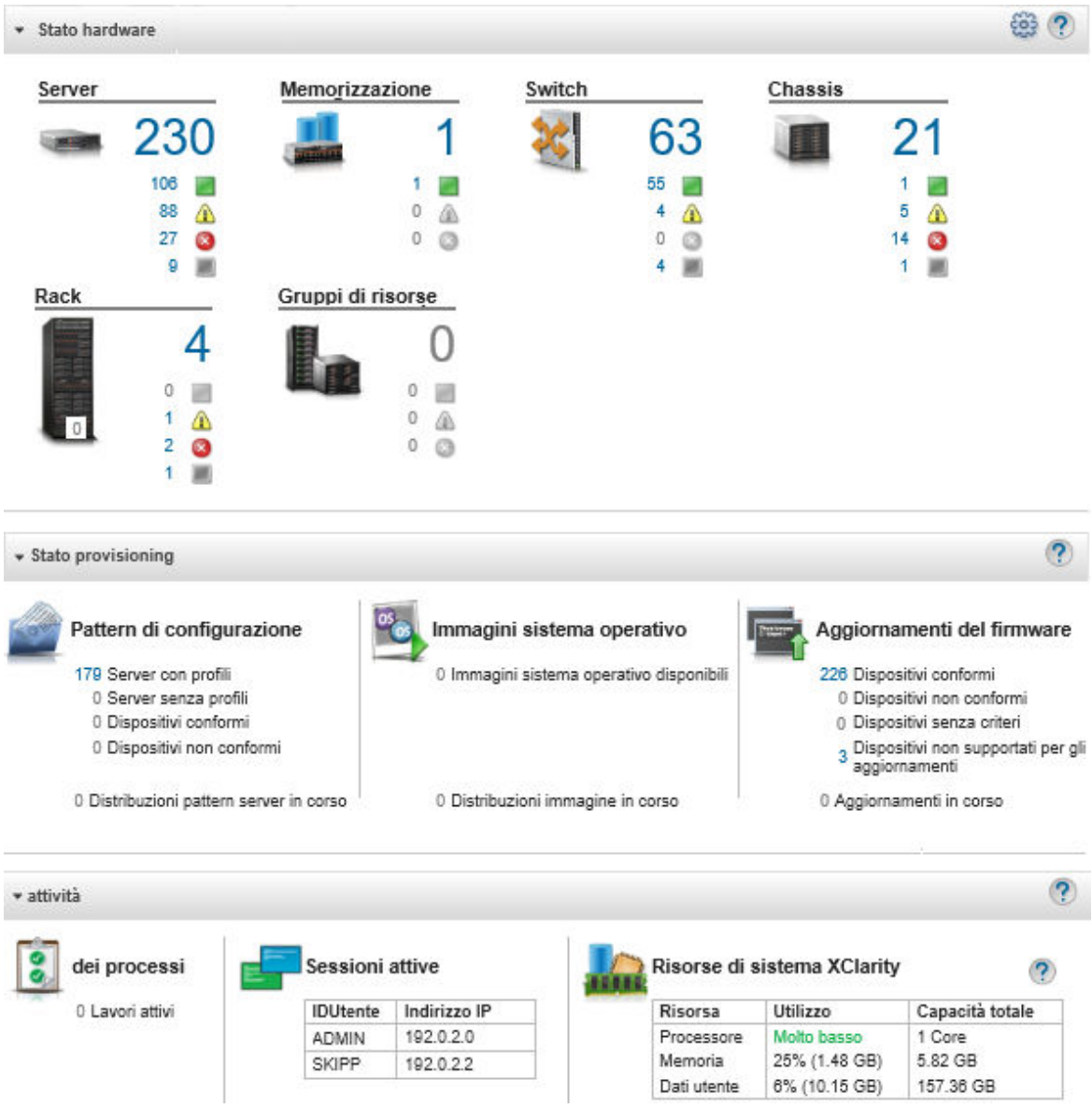
Visualizzazione del riepilogo dell'ambiente in uso

Il dashboard consente di visualizzare lo stato di tutti i dispositivi gestiti, una panoramica delle attività di provisioning e le informazioni sulle risorse e le attività di Lenovo XClarity Administrator.

Ulteriori informazioni:  XClarity Administrator: monitoraggio

Procedura

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Dashboard**.



Passo 2. Espandere lo stato dell'hardware, lo stato del provisioning o la sezione relativa alle attività di amministrazione per ulteriori informazioni su ciascuna di tali aree.

Visualizzazione del riepilogo dello stato dell'hardware

L'area "Stato dell'hardware" consente di visualizzare lo stato di tutti i dispositivi gestiti.

Procedura

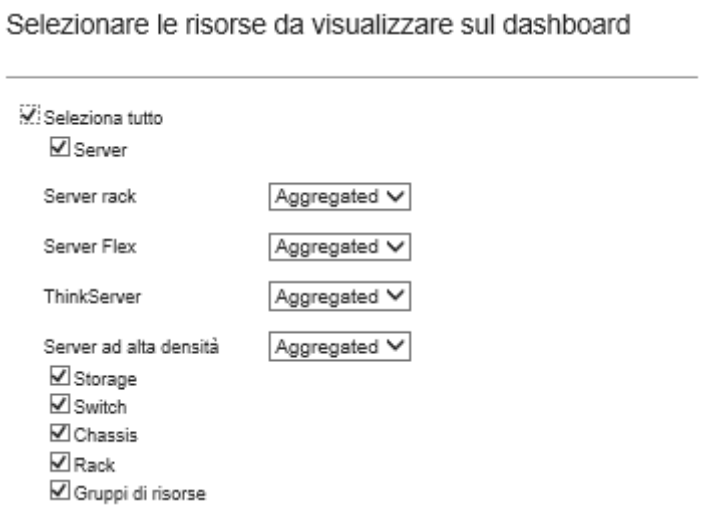
Per ulteriori informazioni su tutti i dispositivi di un determinato tipo, fare clic sul numero elencato sotto al tipo di dispositivo.

Per visualizzare più informazioni solo sui dispositivi di un determinato tipo e stato, fare clic sul numero accanto a ciascuna icona di stato.

- **Server**. Visualizza il numero totale di server (nodi di elaborazione, server rack e server tower) gestiti da XClarity Administrator e il numero di server con stato Normale, Avvertenza e Critico. Per ulteriori informazioni, vedere Visualizzazione dello stato di un server gestito.

- **Storage**. Visualizza il numero totale di dispositivi di storage gestiti da XClarity Administrator e il numero di dispositivi di storage con stato Normale, Avvertenza e Critico. Per ulteriori informazioni, vedere Visualizzazione dello stato dei dispositivi di storage.
- **Switch**. Visualizza il numero totale di RackSwitch e di switch Flex System gestiti da XClarity Administrator, nonché il numero di switch con stato Normale, Avvertenza e Critico. Per ulteriori informazioni, vedere Visualizzazione dello stato degli switch.
- **Chassis**. Visualizza il numero totale di chassis Flex gestiti da XClarity Administrator e il numero di chassis Flex con stato Normale, Avvertenza e Critico. Per ulteriori informazioni, vedere Visualizzazione dello stato di uno chassis gestito.
- **Rack**. Visualizza il numero di rack creati in XClarity Administrator e il numero di rack che includono dispositivi con stato Normale, Avvertenza e Critico più elevato. Per ulteriori informazioni, vedere Visualizzazione dello stato dei dispositivi di un rack.
- **Gruppi di risorse**. Visualizza il numero di gruppi di risorse gestite da XClarity Administrator e il numero di gruppi di risorse che includono dispositivi con stato Normale, Avvertenza e Critico più elevato. Per ulteriori informazioni, vedere Visualizzazione dello stato dei dispositivi in un gruppo di risorse.

Per personalizzare le risorse hardware visualizzate nel dashboard, fare clic sull'icona **Personalizza** (). È possibile scegliere i tipi di dispositivi che si desidera mostrare o nascondere. È inoltre possibile scegliere se aggregare i server in un unico riepilogo, visualizzare i riepiloghi separati per ciascun tipo di server (rack e tower, Flex System, ThinkServer e NeXtScale) oppure omettere tipi specifici di server.



Visualizzazione del riepilogo dello stato del provisioning

L'area "Stato del provisioning" fornisce un riepilogo di tutte le attività associate ai dispositivi di provisioning.

Procedura

- **Pattern di configurazione**. Visualizza le informazioni dettagliate sul numero di server con profili, incluse le seguenti statistiche.

  Nota: Se il server di gestione non è conforme alla licenza, tutti i valori sono 0 (vedere Installazione della licenza di abilitazione di tutte le funzionalità nella documentazione online di XClarity Administrator).

  – Il numero di server conformi al rispettivo profilo del server. È possibile fare clic sul numero per visualizzare la pagina "Pattern di configurazione: profili dei server" con un elenco di server conformi.

- Il numero di server non conformi al rispettivo profilo del server. È possibile fare clic sul numero per visualizzare la pagina "Pattern di configurazione: profili dei server" con un elenco di server non conformi.
- Il numero di dispositivi per cui lo stato di conformità è sconosciuto. È possibile fare clic sul numero per visualizzare la pagina "Pattern di configurazione: profili dei server" con conformità sconosciuta.

  Nota: Lo stato di conformità è sconosciuto, in genere dopo una distribuzione parziale del profilo, quando Lenovo XClarity Administrator non ha raccolto le informazioni di configurazione dal server. Aggiornare l'inventario del server o visitare nuovamente la pagina dei dettagli del profilo del server per forzare la raccolta delle informazioni di configurazione dal server.
- Il numero di server assegnati a un profilo del server. È possibile fare clic sul numero per visualizzare la pagina "Pattern di configurazione: profili dei server" con un elenco di server con profili.
- Il numero di server non assegnati a un profilo del server. È possibile fare clic sul numero per visualizzare la pagina "Pattern di configurazione: pattern server" con un elenco di pattern dei server che possono essere distribuiti ai server senza profili.
- Il numero di pattern dei server attualmente in fase di distribuzione.

Per visualizzare i dati di tendenza dei pattern di configurazione, fare clic su **Visualizza dati di tendenza** (vedere Monitoraggio delle tendenze in stato di provisioning).

Per ulteriori informazioni sui pattern di configurazione e i profili dei server, vedere Configurazione dei server mediante i pattern di configurazione.

- **Immagini sistema operativo**. Visualizza i dettagli sulle distribuzioni del sistema operativo, incluse le seguenti statistiche.

  Nota: Se il server di gestione non è conforme alla licenza, tutti i valori sono 0 (vedere Installazione della licenza di abilitazione di tutte le funzionalità nella documentazione online di XClarity Administrator).
  - Numero di immagini del sistema operativo nel repository. È possibile fare clic sul numero per visualizzare la pagina Distribuisci sistemi operativi: gestisci immagini sistema operativo con un elenco di sistemi operativi.
  - Il numero di distribuzioni del sistema operativo in corso. È possibile fare clic sul numero per visualizzare la pagina Distribuisci sistemi operativi: distribuisci immagini sistema operativo con un elenco di dispositivi su cui è in corso l'installazione di un sistema operativo.
- **Aggiornamenti firmware**. Visualizza i dettagli sugli aggiornamenti firmware, incluse le seguenti statistiche.
  - Numero di dispositivi conformi. È possibile fare clic sul numero per visualizzare la pagina "Aggiornamenti firmware: Applica/Attiva" con un elenco di dispositivi conformi.
  - Numero di dispositivi non conformi. È possibile fare clic sul numero per visualizzare la pagina "Aggiornamenti firmware: Applica/Attiva" con un elenco di dispositivi non conformi.
  - Numero di dispositivi a cui non sono stati assegnati criteri di conformità del firmware. È possibile fare clic sul numero per visualizzare la pagina "Aggiornamenti firmware: Applica/Attiva" con un elenco di dispositivi privi di criteri di conformità.

    Da questa pagina, è possibile assegnare a ciascun dispositivo dei criteri di conformità del firmware, selezionando un criterio dalla colonna **Criterio di conformità assegnato**.
  - Il numero di dispositivi per cui gli aggiornamenti non sono supportati. È possibile fare clic sul numero per visualizzare la pagina "Aggiornamenti firmware: Applica/Attiva" con un elenco di dispositivi per cui gli aggiornamenti non sono supportati.
  - Numero di aggiornamenti in corso.

– Il numero di dispositivi con firmware in sospeso. È possibile fare clic sul numero per visualizzare la pagina "Aggiornamenti firmware: Applica/Attiva" con un elenco di dispositivi per cui l'attivazione degli aggiornamenti è in sospeso.

Per visualizzare i dati di tendenza degli aggiornamenti firmware, fare clic su **Visualizza dati di tendenza** (vedere Monitoraggio delle tendenze in stato di provisioning).

Per ulteriori informazioni su aggiornamenti firmware e i criteri di conformità, vedere Aggiornamento del firmware sui dispositivi gestiti.

Visualizzazione del riepilogo delle attività di Lenovo XClarity Administrator

L'area "Attività" di XClarity Administrator consente di visualizzare le informazioni su processi attivi, sessioni attive e risorse di sistema di XClarity Administrator.

Procedura

- **Processi**. Visualizza il numero di processi attivi attualmente in corso. Per maggiori informazioni sui processi, vedere Monitoraggio dei processi.
- **Sessioni attive**. Visualizza l'ID utente e l'indirizzo IP per ogni sessione attiva di XClarity Administrator. Per maggiori informazioni sugli utenti, vedere Gestione degli account utente.
- **Utilizzo delle risorse**. Visualizza l'utilizzo di processore e memoria, nonché la capacità dei dischi del sistema host e le condivisione remote dei file. Per ulteriori informazioni sulle risorse del sistema, vedere Monitoraggio delle risorse di sistema.

Monitoraggio delle risorse di sistema

È possibile determinare l'utilizzo di processore e memoria, nonché la capacità dei dischi del sistema host dalla pagina "Dashboard".

Prima di iniziare

Devono essere rispettati i seguenti *requisiti minimi* per XClarity Administrator. A seconda delle dimensioni dell'ambiente e dell'utilizzo di Pattern di configurazione, potrebbero essere richieste ulteriori risorse per assicurare prestazioni ottimali.

- Due microprocessori virtuali
- 8 GB di memoria
- 192 GB di storage che verranno utilizzati dall'appliance virtuale XClarity Administrator.
- Da visualizzare con una risoluzione minima di 1.024 pixel in larghezza (XGA)

Nella seguente tabella sono elencate le configurazioni minime consigliate per un determinato numero di dispositivi. Tenere presente che se si esegue la configurazione minima, i tempi di completamento delle attività di gestione potrebbero essere più lunghi del previsto. Per le attività di provisioning, come distribuzione del sistema operativo, aggiornamenti firmware e configurazione dei server, potrebbe essere necessario aumentare temporaneamente le risorse.

Numero di dispositivi gestiti	Configurazione memoria/CPU virtuale
0-100 dispositivi	2 vCPU, 8 GB di RAM
100-200 dispositivi	4 vCPU, 10 GB di RAM
200-400 dispositivi	6 vCPU, 12 GB di RAM
400-600 dispositivi	8 vCPU, 16 GB di RAM

Numero di dispositivi gestiti	Configurazione memoria/CPU virtuale
600-800 dispositivi	10 vCPU, 20 GB di RAM
800-1.000 dispositivi	12 vCPU, 24 GB di RAM

Nota:

- Una singola istanza XClarity Administrator può supportare fino a 1.000 dispositivi.
- Per i suggerimenti più recenti e ulteriori considerazioni sulle prestazioni, vedere XClarity Administrator: guida alle prestazioni (white paper).
- In base alla dimensione dell'ambiente gestito e dei pattern di utilizzo dell'installazione, potrebbe essere necessario aggiungere ulteriori risorse per garantire prestazioni accettabili. Se spesso viene riscontrato un utilizzo elevato o molto elevato del processore nel dashboard delle risorse di sistema, considerare la possibilità di aggiungere 1-2 core di processore virtuale. Se l'utilizzo minimo della memoria supera l'80%, considerare la possibilità di aggiungere 1-2 GB di RAM. Se il sistema rientra tra le configurazioni definite nella tabella, si consiglia di eseguire la macchina virtuale per un periodo maggiore di tempo per valutare le prestazioni del sistema.
- Per informazioni su come liberare spazio su disco eliminando le risorse di XClarity Administrator non più necessarie, vedere Gestione dello spazio su disco.

Procedura

Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Dashboard**.

L'utilizzo delle risorse del sistema host è riportato nella sezione "Attività" di XClarity Administrator.

Processore

La misurazione dell'utilizzo indica il numero di processi XClarity Administrator a cui accedono contemporaneamente i processori dell'host.

Suggerimento: talvolta, il valore di picco di utilizzo potrebbe essere "Alto" o "Molto Alto". Se l'utilizzo resta su questo livello per più di 30 minuti, consultare il log dei processi per verificare se sono presenti processi a esecuzione prolungata (vedere Monitoraggio dei processi).

La misurazione della capacità totale indica il numero processori disponibili sull'host.

Memoria

La misurazione dell'utilizzo indica la quantità di memoria attualmente utilizzata da XClarity Administrator.

La misurazione della capacità totale indica la quantità totale di memoria disponibile sull'host.

Dati utente

La misurazione dell'utilizzo indica lo spazio su disco attualmente utilizzato da XClarity Administrator sul sistema host.

La misurazione della capacità totale indica la quantità totale di spazio (utilizzato e non utilizzato) allocato per i dati utente, come i sistemi operativi e gli aggiornamenti firmware.

Per ulteriori informazioni sulla gestione dello spazio su disco, vedere Gestione dello spazio su disco.

Attenzione: Se le risorse allocate non sono sufficienti per gestire il numero corrente di dispositivi gestiti con prestazioni soddisfacenti, considerare la possibilità di aumentare l'allocazione delle risorse. Per ulteriori informazioni sui requisiti hardware consigliati in base al numero di dispositivi gestiti nell'ambiente, vedere Sistemi host supportati nella documentazione online di XClarity Administrator.

Monitoraggio delle tendenze in stato di provisioning

Lenovo XClarity Administrator raccoglie regolarmente lo stato del provisioning, come conformità e processi attivi per gli aggiornamenti firmware e i pattern di configurazione per tutti i dispositivi gestiti, in modo da monitorare le tendenze per un determinato periodo di tempo.

Informazioni su questa attività

È necessario disporre dell'autorità **lxc_admin** o **lxc-supervisor** per visualizzare i dati delle tendenze.

Vengono raccolti i seguenti dati:

- **Aggiornamenti firmware**
  - **Dispositivi conformi**. Numero di dispositivi conformi, con i rispettivi criteri di conformità del firmware assegnati.
  - **Dispositivi non conformi**. Numero di dispositivi non conformi, con i rispettivi criteri di conformità del firmware assegnati.
  - **Dispositivi senza criteri**. Numero di dispositivi a cui non sono stati assegnati criteri di conformità del firmware
  - **Dispositivi non supportati per gli aggiornamenti**. Numero di dispositivi per cui gli aggiornamenti firmware non sono supportati
  - **Aggiornamenti in corso**. Numero di dispositivi per cui gli aggiornamenti firmware sono in corso
- **Pattern di configurazione**
  - **Server con profili**. Numero di dispositivi con un profilo del server assegnato
  - **Server senza profili**. Numero di dispositivi senza un profilo del server assegnato
  - **Server conformi**. Numero di dispositivi conformi al profilo del server assegnato
  - **Server non conformi**. Numero di dispositivi non conformi al profilo del server assegnato
  - **Pattern server in corso**. Numero di dispositivi per cui gli aggiornamenti dei pattern di configurazione sono in corso

Procedura

Completare le seguenti operazioni per visualizzare le tendenze in stato di provisioning.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Dashboard** per visualizzare la pagina Dashboard.

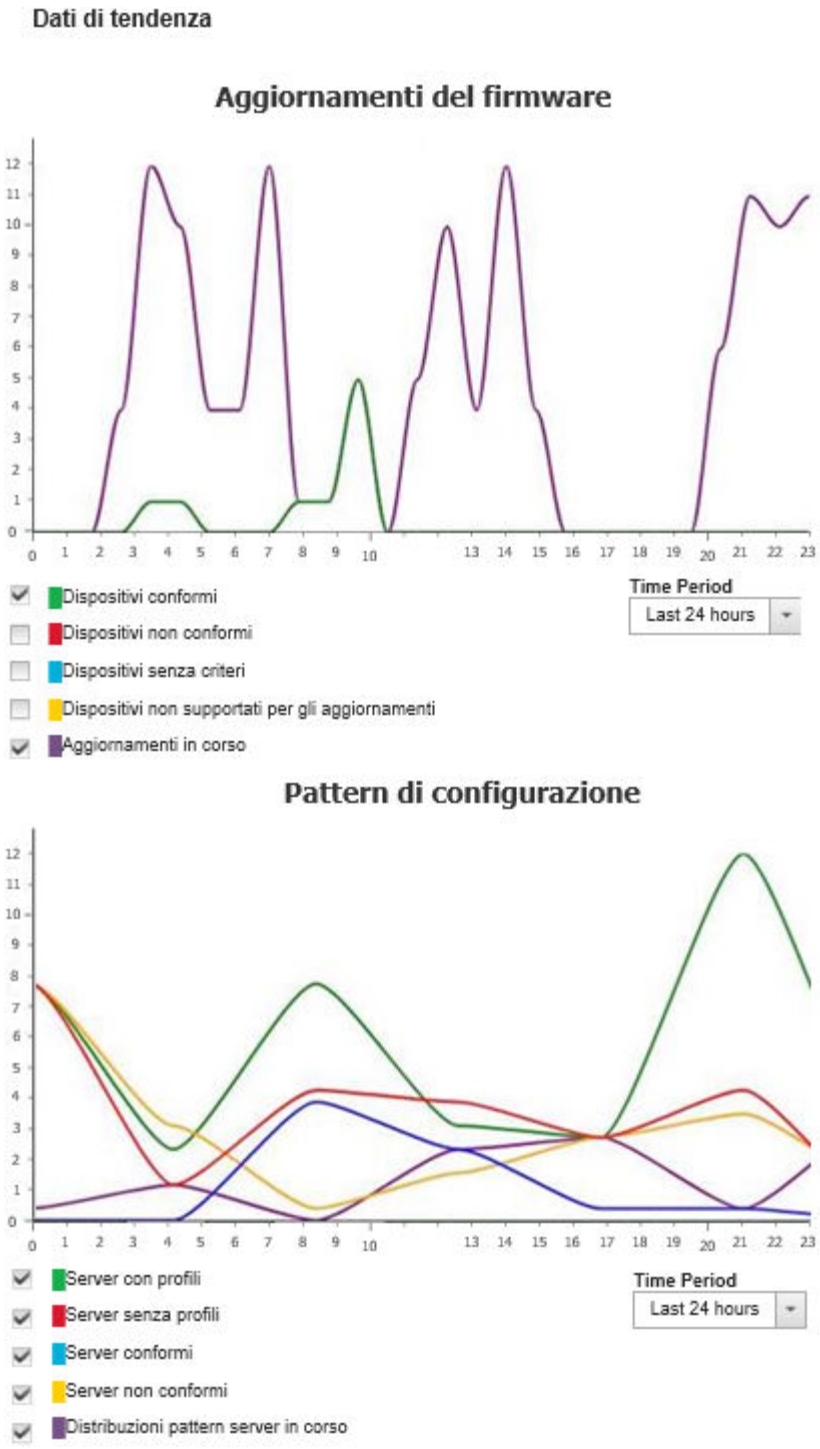
Passo 2. Fare clic sul collegamento **Dati di tendenza** per visualizzare la finestra di dialogo "Impostazioni soglia".

Passo 3. Deselezionare o selezionare i dati che si desidera visualizzare.

Passo 4. Selezionare il periodo di tempo che si desidera visualizzare.

- **24 ore**. Visualizza i dati delle ultime 24 ore. Ogni punto dati è una media per un periodo di 1 ora.
- **1 mese**. Visualizza i dati degli ultimi 30 giorni. Ogni punto dati è una media per un periodo di 24 ore.

I dati di tendenza vengono mostrati come un grafico per il periodo di tempo selezionato.



Monitoraggio delle metriche cronologiche

Lenovo XClarity Administrator raccoglie regolarmente i dati delle metriche per i dispositivi ThinkSystem e ThinkAgile gestiti, in modo da poter analizzare lo stato corrente dell'ambiente.

Prima di iniziare

Le metriche storiche sono supportate solo per i server ThinkSystem (ad eccezione di SR635, SR645, SR655 e SR665).

Sono supportate solo le unità SSD nei server ThinkAgile e ThinkSystem (ad eccezione di SR635 e SR655) con firmware XCC rilasciato dopo aprile 2019.

I driver SATA integrati non sono supportati.

Le unità NVMe devono supportare la specifica NVMe-MI (NVMe Management Interface).

Informazioni su questa attività

Vengono raccolte le metriche seguenti.

- **Monitoraggio SSD** Questa scheda del report include le statistiche e i grafici seguenti.
  - Numero totale di unità SSD nei dispositivi gestiti (in base all'ambito).
  - Numero di unità SSD analizzate
  - Numero di unità SSD non idonee per l'analisi
  - Grafico circolare che mostra il numero di dispositivi con SSD dotati di durata residua in un intervallo specifico.
    - Durata residua <= 10%. Numero di unità SSD con durata residua massima del 10%
    - Durata residua 11-50%. Numero di unità SSD con durata residua pari a 11-50%
    - Durata residua 51-100%. Numero di unità SSD con durata residua superiore al 50%
- **Utilizzo del sistema** Questa scheda del report include le statistiche e i grafici seguenti.
  - L'utilizzo corrente del processore, in percentuale
  - L'utilizzo corrente della memoria, in percentuale
  - Grafico a linee che mostra l'utilizzo del processore e della memoria nel tempo
- **Consumo energetico** Questa scheda del report include le statistiche e i grafici seguenti.
  - L'ingresso di alimentazione totale corrente per tutti gli alimentatori, in watt
  - Un grafico a linee che mostra l'ingresso totale dell'alimentazione nel tempo
- **Temperatura dispositivo** Questa scheda del report include le statistiche e i grafici seguenti.
  - La temperatura massima corrente dell'aria in ingresso, in Celsius
  - Un grafico a linee che mostra la temperatura massima nel tempo

È possibile passare il mouse su ogni linea colorata nel grafico circolare, su ciascun punto nel grafico a linee o nel numero accanto a ogni metrica per ottenere ulteriori informazioni sulla metrica. È possibile visualizzare o nascondere le metriche nel grafico facendo clic sull'icona a colori nella legenda. È inoltre possibile fare clic su un numero collegato o sull'opzione nell'icona **Impostazioni** () nell'angolo superiore destro della scheda per visualizzare un elenco di tutti i dispositivi con metriche sull'utilizzo che soddisfano i criteri selezionati.

Procedura

Completare le seguenti operazioni per visualizzare il diagramma di flusso per un'attività specifica.

Passo 1. Sulla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Metriche storiche** per visualizzare la pagina Metriche storiche con schede di riepilogo per ogni tipo di metrica.

Passo 2. Impostare l'ambito su tutti o su un gruppo specifico di dispositivi.

Impostazione dei dispositivi in modalità di manutenzione

Quando un dispositivo è in modalità di manutenzione, Lenovo XClarity Administrator esclude tutti gli eventi e gli avvisi per tale dispositivo da tutte le pagine in cui sono visualizzati gli eventi e gli avvisi. Gli avvisi esclusi vengono comunque registrati ma nascosti alla vista.

Informazioni su questa attività

Sono esclusi soltanto gli eventi e gli avvisi generati per un dispositivo mentre questo è in modalità di manutenzione. Gli eventi e gli avvisi prima che il dispositivo venisse messo in modalità di manutenzione vengono invece visualizzati.

La riattivazione di un dispositivo gestito precedentemente impostato in modalità di manutenzione potrebbe rendere obsoleto l'inventario per tale dispositivo. In caso di anomalie, aggiornare manualmente l'inventario dalla pagina del dispositivo selezionando il dispositivo stesso e facendo clic su **Tutte le azioni → Inventario → Aggiorna inventario**.

Procedura

Completare una delle seguenti operazioni per impostare i dispositivi in modalità di manutenzione.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Amministrazione → Assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.

Passo 2. Fare clic su **Azioni endpoint** nel riquadro di navigazione sinistro per visualizzare la pagina Azioni endpoint.

Passo 3. Selezionare uno o più dispositivi da impostare in modalità di manutenzione.

Passo 4. Fare clic su **Azioni → Manutenzione** per visualizzare la finestra di dialogo Modalità di manutenzione.

Passo 5. Selezionare la data e l'ora per la riattivazione del dispositivo.

Selezionare **Indefinita** se non si desidera riattivare il dispositivo.

Passo 6. Fare clic su **Conferma**. La colonna di manutenzione nella tabella viene modificata in Sì per tale dispositivo.

Al termine

Una volta completata la manutenzione del dispositivo, è possibile riattivare il dispositivo selezionandolo e facendo clic su **Azioni → Manutenzione**, quindi facendo clic su **Disattiva manutenzione** nella finestra di dialogo. Se il dispositivo non viene manualmente riattivato (rimesso in funzione), viene automaticamente impostato in modalità di servizio allo scadere del tempo specificato.

Gestione degli avvisi

Gli *avvisi* sono condizioni hardware o di gestione che richiedono l'analisi e l'intervento dell'utente. Lenovo XClarity Administrator esegue il polling dei dispositivi gestiti in modo asincrono e visualizza avvisi ricevuti da tali dispositivi.

Ulteriori informazioni: XClarity Administrator: monitoraggio

Informazioni su questa attività

Di norma, quando si riceve un avviso, un evento corrispondente viene archiviato nel log eventi. È possibile che a un avviso non corrisponda alcun evento nel log eventi (nonostante il wrapping del log). Ad esempio, gli eventi che si verificano prima di gestire uno chassis non vengono visualizzati nel log eventi. Tuttavia, gli avvisi per lo chassis vengono visualizzati nel log avvisi poiché Lenovo XClarity Administrator esegue il polling di CMM dopo che lo chassis è stato gestito.

Visualizzazione di avvisi attivi

È possibile visualizzare l'elenco di tutti gli avvisi hardware e di gestione attivi.

Informazioni su questa attività

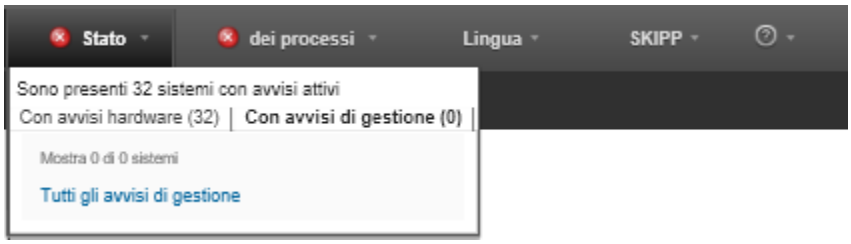
Nota: gli avvisi per i dispositivi Lenovo Storage vengono visualizzati solo in inglese, anche se le impostazioni locali di Lenovo XClarity Administrator sono configurate su un'altra lingua. Se necessario, utilizzare un sistema di traduzione esterno per tradurre i messaggi manualmente.

Procedura

Per visualizzare gli avvisi attivi, completare una di queste procedure.

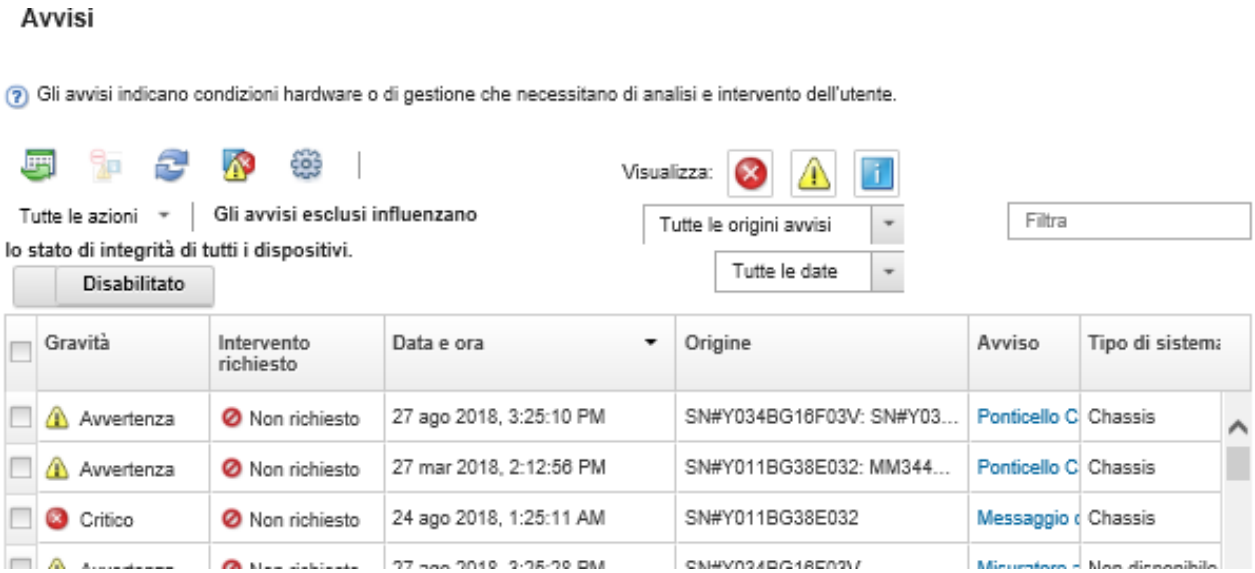
- Per visualizzare solo gli avvisi per i dispositivi gestiti (noti come *avvisi hardware):*
  1. Nella barra del titolo di XClarity Administrator fare clic sull'elenco a discesa **Stato** per visualizzare un riepilogo degli avvisi hardware e di gestione.
  2. Fare clic sulla scheda **Con avvisi hardware** per visualizzare un riepilogo degli avvisi per ogni dispositivo gestito.

  3. Passare il cursore su un dispositivo elencato in tale scheda per visualizzare l'elenco dei relativi avvisi.
  4. Fare clic sul collegamento **Tutti gli avvisi hardware** per visualizzare la pagina Avvisi con un elenco filtrato di tutti gli avvisi hardware.
- Per visualizzare solo gli avvisi di XClarity Administrator (noti come *avvisi di gestione*):
  1. Nella barra del titolo di XClarity Administrator fare clic sull'elenco a discesa **Stato** per visualizzare un riepilogo degli avvisi hardware e di gestione.
  2. Fare clic sulla scheda **Con avvisi di gestione** per visualizzare un riepilogo di tutti i CMM e degli avvisi di XClarity Administrator.



3. Passare il cursore su un dispositivo elencato in tale scheda per visualizzare l'elenco dei relativi avvisi.
4. Fare clic sul collegamento **Tutti gli avvisi di gestione** per visualizzare la pagina Avvisi con un elenco filtrato di tutti gli avvisi del CMM e di XClarity Administrator.

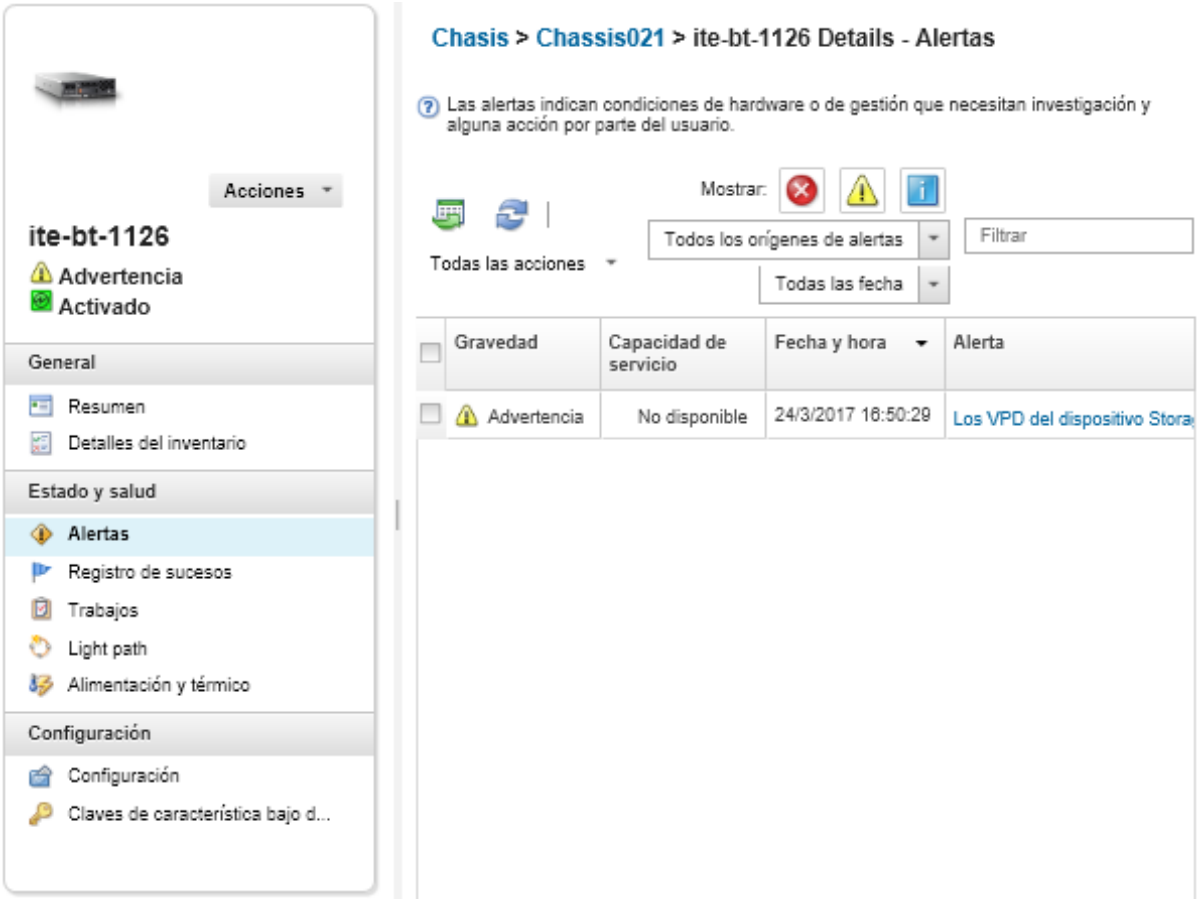
- Per visualizzare tutti gli avvisi in XClarity Administrator, fare clic su **Monitoraggio → Avvisi** nella barra dei menu di XClarity Administrator. Verrà visualizzata la pagina Avvisi con l'elenco di tutti gli avvisi attivi.



- Per visualizzare gli avvisi per uno specifico dispositivo:
  1. Nella barra dei menu di XClarity Administrator fare clic su **Hardware** e selezionare un tipo di dispositivo. Verrà visualizzata una pagina contenente una vista tabulare di tutti i dispositivi gestiti di tale tipo. Ad esempio, fare clic su **Hardware → Server** per visualizzare la pagina Server.
  2. Fare clic su uno specifico dispositivo per visualizzare la pagina Riepilogo per il dispositivo.
  3. In Stato e integrità fare clic su **Avvisi** per visualizzare l'elenco di tutti gli avvisi associati a tale dispositivo.

     Nota: nella colonna Intervento richiesto è possibile che venga visualizzato il messaggio "Non disponibile" se:

     – L'avviso sul dispositivo è stato visualizzato prima che XClarity Administrator iniziasse a gestirlo.
     – Il wrapping del log eventi ha fatto sì che l'evento associato a tale avviso non sia più nel log eventi.



Risultati

Dalla pagina Avvisi è possibile completare le seguenti azioni:

- Aggiornare l'elenco degli avvisi facendo clic sull'icona **Aggiorna** ( ).

  Suggerimento: Se vengono rilevati nuovi avvisi, il log avvisi si aggiorna automaticamente ogni 30 secondi.
- Visualizzare informazioni su un avviso specifico (inclusa una descrizione e l'intervento dell'utente) e sul dispositivo da cui ha avuto origine l'avviso (come l'UUID) facendo clic sul collegamento nella colonna **Avviso**. Verrà visualizzata una finestra di dialogo con dettagli e informazioni sulle proprietà degli avvisi.

  Nota: Se la descrizione e le azioni di ripristino di un avviso non sono visualizzate nella scheda **Dettagli**, andare al Documentazione online di Lenovo Flex System e cercare l'ID dell'avviso (ad esempio, `FQXHMSE0004G`). Nel sito Web sono sempre disponibili le informazioni più aggiornate.
- Per impostazione predefinita, gli avvisi esclusi non incidono sullo stato dell'integrità dei dispositivi gestiti. È possibile consentire agli avvisi esclusi di incidere sullo stato dell'integrità dei dispositivi gestiti dalla pagina Avvisi, facendo clic sull'interruttore per abilitare **Gli eventi esclusi incidono sullo stato di integrità di tutti i dispositivi**.
- È possibile impostare le preferenze delle soglie per la generazione di un avviso e di un evento quando un determinato valore, come la durata di un'unità SSD di un server ThinkSystem o ThinkServer, supera un livello di avvertenza o critico (vedere Impostazione delle preferenze delle soglie per la generazione di eventi e avvisi).
- Esportare il log avvisi facendo clic sull'icona **Esporta come CSV** ( ).

Nota: Per i timestamp nel log esportato viene utilizzata l'ora locale specificata dal browser Web.

- Escludere avvisi specifici da tutte le pagine in cui sono visualizzati gli avvisi (vedere Esclusione di avvisi).
- Limitare l'elenco di avvisi visualizzati nella pagina corrente:
  - Mostrare o nascondere gli avvisi di una gravità specifica facendo clic sulle seguenti icone:
    - Icona **Avvisi critici** ()
    - Icona **Avvisi di avvertenza** ()
    - Icona **Avvisi informativi** ()
  - Mostrare solo avvisi di origini specifiche. È possibile scegliere una delle seguenti opzioni dall'elenco a discesa:
    - Tutte le origini avvisi
    - Eventi hardware
    - Eventi di gestione
    - Eventi centro di assistenza
    - Eventi manutenibili cliente
    - Eventi non manutenibili
  - Mostrare solo avvisi con data e ora specifiche. È possibile scegliere una delle seguenti opzioni dall'elenco a discesa:
    - Tutte le date
    - Due ore precedenti
    - 24 ore precedenti
    - Scorsa settimana
    - Scorso mese
  - Elencare solo gli avvisi che contengono testo specifico immesso nel campo **Filtro**.
  - Ordinare gli avvisi per colonna facendo clic su un'intestazione di colonna.

Esclusione di avvisi

Avvisi specifici ritenuti inutili dall'utente possono essere esclusi da tutte le pagine in cui vengono visualizzati. Gli avvisi esclusi rimangono continuano a essere presenti nel log ma non vengono visualizzati in nessuna delle pagine dedicate agli avvisi, incluse le visualizzazioni del log e lo stato del dispositivo.

Informazioni su questa attività

Gli avvisi esclusi vengono nascosti a tutti gli utenti e non solo all'utente che imposta la configurazione.

È possibile impostare i dispositivi in modalità di manutenzione, in modo da escludere tutti gli eventi e gli avvisi relativi a questi dispositivi (vedere Impostazione dei dispositivi in modalità di manutenzione).

Restrizione: solo gli utenti con privilegi di amministratore possono escludere o ripristinare gli avvisi.

Importante: se si escludono gli avvisi di stato, lo stato del dispositivo nel riepilogo dei dispositivi e nelle pagine dei dettagli rimarrà inalterato.

Procedura

Per escludere avvisi dal log avvisi, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Monitoraggio → Avvisi**. Verrà visualizzata la pagina Avvisi.

Passo 2. Selezionare gli avvisi da escludere e fare clic sull'icona **Escludi avvisi** (). Verrà visualizzata la finestra di dialogo Escludi avvisi.

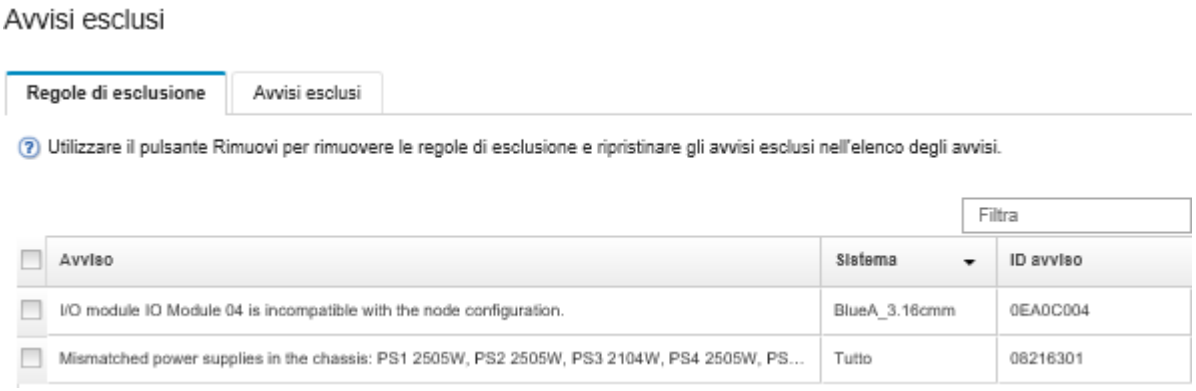
Passo 3. Selezionare una delle seguenti opzioni:

- **Escludi avvisi selezionati da tutti i sistemi**. Esclude gli avvisi selezionati da tutti i dispositivi gestiti.
- **Escludi avvisi solo dai sistemi nell'ambito dell'istanza selezionata**. Esclude gli avvisi selezionati dai dispositivi gestiti a cui si applicano.

Passo 4. Fare clic su **Salva**.

Al termine

Quando si escludono avvisi, Lenovo XClarity Administrator crea regole di esclusione basate sulle informazioni fornite. È possibile visualizzare un elenco di regole di esclusione e di avvisi esclusi dalla pagina Avvisi facendo clic sull'icona **Mostra avvisi esclusi/confermati** (). Nella finestra di dialogo Avvisi esclusi/confermati fare clic sulla scheda **Regole di esclusione** per visualizzare l'elenco delle regole di esclusione oppure fare clic sulla scheda **Avvisi esclusi** per visualizzare l'elenco degli avvisi esclusi.



Per impostazione predefinita, gli avvisi esclusi non incidono sullo stato dell'integrità dei dispositivi gestiti. È possibile consentire agli avvisi esclusi di incidere sullo stato dell'integrità dei dispositivi gestiti dalla pagina Avvisi, facendo clic sull'interruttore per abilitare **Mostra avvisi esclusi/confermati**.

È possibile ripristinare gli avvisi esclusi nel log avvisi rimuovendo la regola di esclusione appropriata. Per rimuovere una regola di esclusione, fare clic sull'icona **Mostra eventi esclusi** () per visualizzare la relativa finestra di dialogo, selezionare le regole di esclusione o l'avviso escluso da ripristinare e fare clic su **Rimuovi**.

Risoluzione di un avviso

Lenovo XClarity Administrator fornisce informazioni sulle azioni appropriate da eseguire per risolvere un avviso.

Procedura

Per risolvere un avviso, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Monitoraggio → Avvisi** per visualizzare la pagina Avvisi.

Passo 2. Individuare l'avviso nel log avvisi.

Passo 3. Fare clic sul collegamento nella colonna **Avviso** per visualizzare informazioni sull'avviso (inclusa una descrizione e le azioni di ripristino) e le proprietà del dispositivo da cui l'avviso ha avuto origine (come l'UUID).

Passo 4. Per risolvere l'avviso, attenersi alle azioni di ripristino elencate nella scheda **Dettagli**. L'esempio seguente mostra le azioni di ripristino di un evento.

Modificare l'impostazione del criterio di sicurezza sullo chassis gestito di riferimento affinché corrisponda al criterio di sicurezza corrente sul server di gestione.

Per modificare il criterio di sicurezza nello chassis, aprire una sessione dell'interfaccia della riga di comando su Chassis Management Module (CMM) ed eseguire uno dei seguenti comandi:

- Per modificare il livello di criteri di sicurezza in `Secure`:
  ```
  security -p secure -T mm[p]
  ```
- Per modificare il livello di criteri di sicurezza in `Legacy`:
  ```
  security -p legacy -T mm[p]
  ```

Nota: Se la descrizione e le azioni di ripristino di un avviso non sono visualizzate nella scheda **Dettagli**, andare al Documentazione online di Lenovo Flex System e cercare l'ID dell'avviso (ad esempio, `FQXHMSE0004G`). Nel sito Web sono sempre disponibili le informazioni più aggiornate.

Se, dopo essersi attenuti alla procedura consigliata, il problema persiste, contattare il Supporto Lenovo.

Conferma degli avvisi

Quando viene confermato un avviso attivo, l'avviso viene elencato nelle pagine in cui vengono visualizzati gli avvisi ma non incide sullo stato di gravità del dispositivo applicabile.

Procedura

Per confermare un avviso, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Monitoraggio → Avvisi**. Verrà visualizzata la pagina Avvisi.

Passo 2. Selezionare gli avvisi da confermare.

Passo 3. Fare clic sull'icona **Avvisi confermati** ( ).

Al termine

- È possibile visualizzare un elenco di avvisi confermati dalla pagina Avvisi facendo clic sull'icona **Mostra avvisi esclusi/confermati** ( ) per visualizzare la finestra di dialogo Avvisi esclusi/confermati e facendo quindi clic sulla scheda **Avvisi confermati**.
- È possibile rimuovere la conferma di un avviso attivo facendo clic sull'icona **Mostra avvisi esclusi/confermati** ( ) per visualizzare la finestra di dialogo Avvisi esclusi/confermati, selezionando la scheda **Avvisi confermati**, scegliere gli avvisi e quindi fare clic sull'icona **Rimuovi conferma** ( ).

Utilizzo degli eventi

Da Lenovo XClarity Administrator è possibile accedere a un log eventi e a un log di controllo.

Ulteriori informazioni: XClarity Administrator: monitoraggio

Informazioni su questa attività

Il *log eventi* fornisce un elenco cronologico di tutti gli eventi di gestione e hardware.

Il *log di controllo* fornisce un record cronologico degli interventi dell'utente, ad esempio il login a Lenovo XClarity Administrator, la creazione di un nuovo utente e la modifica di una password utente. È possibile utilizzare il log di controllo per tenere traccia e documentare l'autenticazione e i comandi nei sistemi IT.

Monitoraggio degli eventi nel log eventi

Il *log eventi* fornisce un elenco cronologico di tutti gli eventi di gestione e hardware.

Informazioni su questa attività

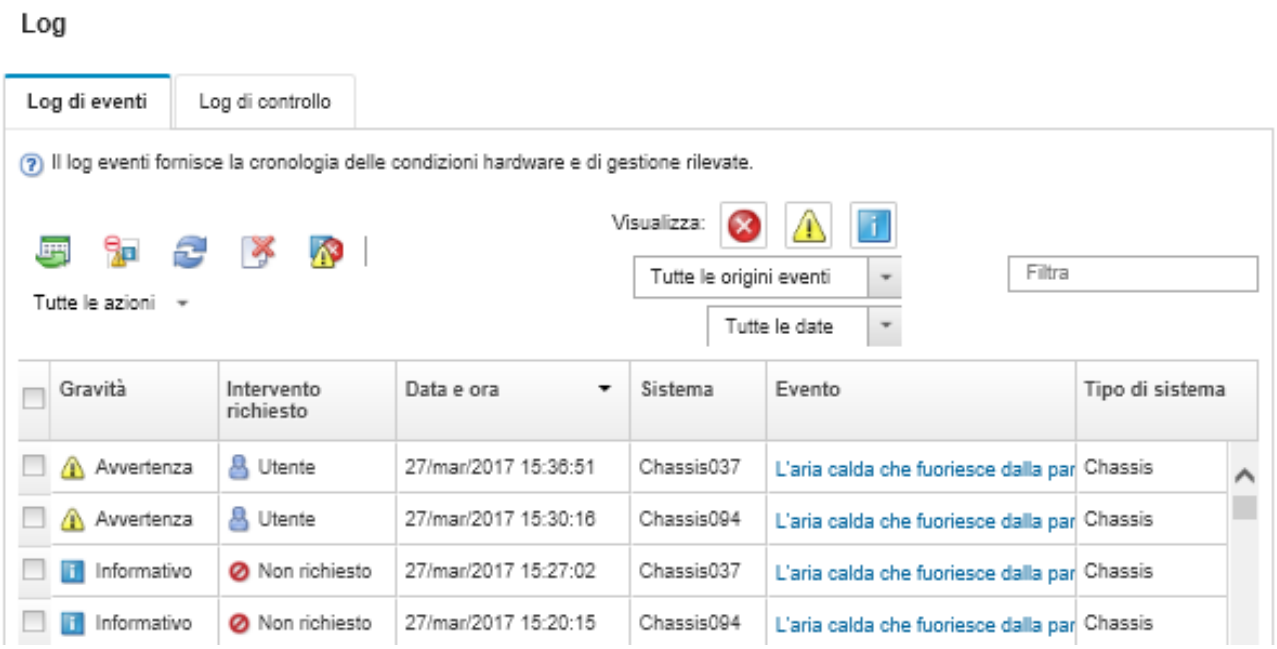
Il log eventi contiene gli eventi informativi e non informativi. Il numero di ciascuno di questi eventi varia finché non viene raggiunto il numero massimo di 50.000 eventi nel log eventi. In quel momento, si registra un massimo di 25.000 eventi informativi e 25.000 eventi non informativi. Inizialmente, ad esempio, nel log eventi sono presenti 0 eventi. Poniamo che vengano ricevuti 20.000 eventi informativi e 30.000 eventi non informativi. Quando viene ricevuto l'evento successivo, l'evento informativo meno recente viene rimosso se un evento non informativo è meno recente. Alla fine il log bilancia gli eventi al fine di contenere 25.000 eventi per ciascun tipo.

Lenovo XClarity Administrator invia un evento quando il log eventi raggiunge l'80% delle dimensioni minime e un altro evento quando la somma dell'evento e dei log di controllo raggiunge il 100% delle dimensioni massime.

Suggerimento: è possibile esportare il log eventi per assicurarsi di avere un record completo di tutti gli eventi hardware e di gestione. Per esportare il log eventi fare clic sull'icona **Esporta come CSV** ( ).

Procedura

Per visualizzare il log eventi, fare clic su **Monitoraggio → Log eventi** dalla barra dei menu di Lenovo XClarity Administrator, quindi sulla scheda **Log eventi**. Viene visualizzata la pagina Log eventi.



La colonna **Intervento richiesto** indica se il dispositivo richiede un intervento. Questa colonna può contenere uno dei seguenti valori:

- **Non richiesto**. L'evento è informativo e non richiede intervento.
- **Utente**. Intraprende l'azione di ripristino appropriata per risolvere il problema.

Per visualizzare le informazioni su un evento specifico, fare clic sul collegamento nella colonna **Evento**. Viene visualizzata una finestra di dialogo con informazioni sulle proprietà del dispositivo che ha inviato l'evento, i dettagli sull'evento e le azioni di ripristino.

- **Supporto**. Se Call Home è abilitato su Lenovo XClarity Administrator, l'evento verrà generalmente inoltrato al Centro assistenza clienti Lenovo a meno che non esista già un ticket di assistenza per lo stesso ID evento per il dispositivo.

  Se Call Home non è abilitato, si consiglia di aprire manualmente un ticket di assistenza per risolvere il problema (vedere Apertura di un ticket di assistenza nella documentazione online Lenovo XClarity Administrator).

Risultati

Dalla pagina Log eventi, procedere come segue:

- Visualizzare l'origine dell'evento facendo clic sul collegamento nella colonna **Origine**.
- Aggiornare l'elenco degli elenchi facendo clic sull'icona **Aggiorna** ( ).

  Suggerimento: il log eventi si aggiorna automaticamente ogni 30 secondi se vengono rilevati nuovi eventi.
- Cancella tutti gli eventi dal log eventi selezionando **Tutte le azioni → Cancella log eventi**.
- Visualizzare i dettagli su un evento specifico facendo clic sul collegamento nella colonna **Evento**, quindi sulla scheda **Dettagli**.
- Esportare il log eventi facendo clic sull'icona **Esporta come CSV** ( ).

  Nota: Per i timestamp nel log esportato viene utilizzata l'ora locale specificata dal browser Web.
- Escludere gli eventi specifici da tutte le pagine in cui vengono visualizzati gli eventi (vedere Esclusione di eventi).
- Restringere l'elenco degli eventi di gestione e hardware visualizzati nella pagina corrente:
  - Mostrare o nascondere gli eventi di una gravità specifica facendo clic sulle seguenti icone dall'elenco a discesa:
    - Icona **Eventi critici** ( )
    - Icona **Eventi di avvertenza** ( )
    - Icona **Eventi informativi** ( )
  - Mostrare solo eventi di fonti specifiche. È possibile scegliere una delle seguenti opzioni dall'elenco a discesa:
    - Tutte le origini avvisi
    - Eventi hardware
    - Eventi di gestione
    - Eventi di manutenzione
    - Eventi manutenibili cliente
    - Eventi non manutenibili
  - Mostrare solo gli eventi con una data e un'ora specifiche. É possibile scegliere una delle seguenti opzioni:
    - Tutte le date
    - 2 ore precedenti
    - 24 ore precedenti
    - Scorsa settimana
    - Scorso mese
    - Custom

Se si seleziona **Personalizzato**, è possibile filtrare gli eventi di gestione e hardware generati tra una data di avvio personalizzata e la data corrente.

- Elencare solo gli eventi che contengono testo specifico immesso nel campo **Filtro**.
- Ordinare gli eventi per colonna facendo clic sull'intestazione di una colonna.

Monitoraggio degli eventi nel log di controllo

Il *log di controllo* fornisce un record cronologico degli interventi dell'utente, ad esempio il login a Lenovo XClarity Administrator, la creazione di un nuovo utente e la modifica di una password utente. È possibile utilizzare il log di controllo per tenere traccia e documentare l'autenticazione e i comandi nei sistemi IT.

Informazioni su questa attività

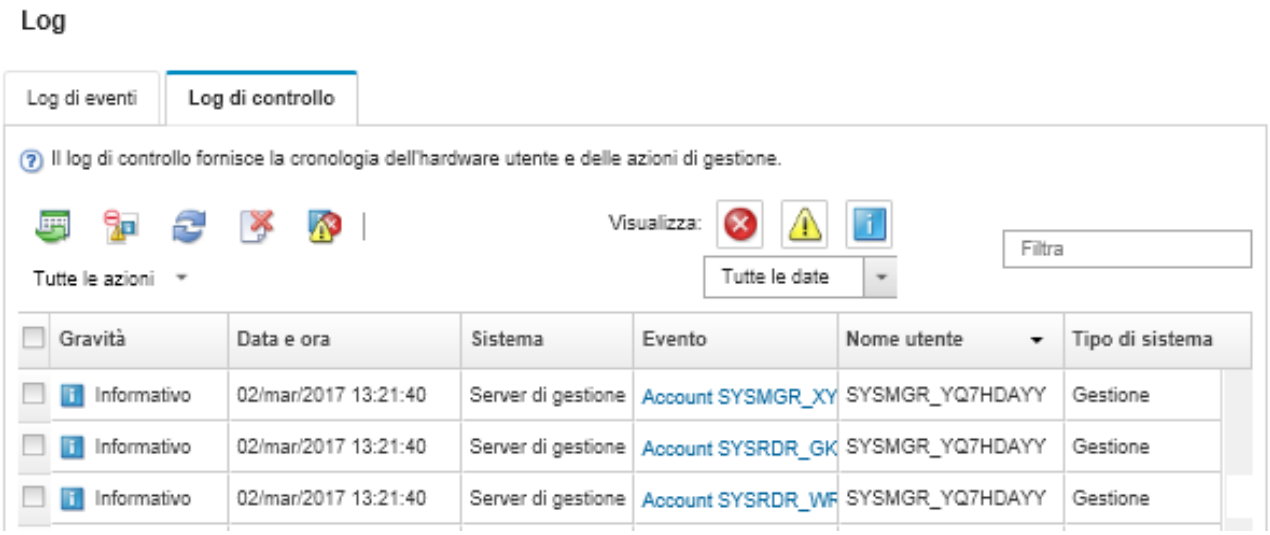
Il log di controllo può contenere un massimo di 50.000 eventi. Quando le dimensioni massime vengono raggiunte, l'evento meno recente nel log viene rimosso e il nuovo evento viene aggiunto al log.

XClarity Administrator invia un evento quando il log di controllo raggiunge l'80% delle dimensioni massime ed un altro evento quando la somma dell'evento e dei log di controllo raggiunge il 100% delle dimensioni massime.

Suggerimento: è possibile esportare il log di controllo per assicurarsi di avere un record completo di tutti gli eventi di controllo. Per esportare il log di controllo fare clic sull'icona **Esporta come CSV** ( ).

Procedura

Per visualizzare il log di controllo, fare clic su **Monitoraggio → Log eventi** dalla barra dei menu di XClarity Administrator, quindi sulla scheda **Log di controllo**. Viene visualizzata la pagina Log di controllo.



Per visualizzare le informazioni su un evento di controllo specifico, fare clic sul collegamento nella colonna **Evento**. Viene visualizzata una finestra di dialogo con informazioni sulle proprietà del dispositivo che ha inviato l'evento, i dettagli sull'evento e le azioni di ripristino.

Risultati

Da questa pagina, è possibile eseguire le seguenti azioni:

- Visualizzare l'origine dell'evento di controllo facendo clic sul collegamento nella colonna **Origine**.

- Aggiornare l'elenco degli eventi di controllo facendo clic sull'icona **Aggiorna** ().

  Suggerimento: il log eventi si aggiorna automaticamente ogni 30 secondi se vengono rilevati nuovi eventi.
- Visualizzare i dettagli su un evento di controllo specifico facendo clic sul collegamento nella colonna **Evento**, quindi sulla scheda **Dettagli**.
- Esportare il log di controllo facendo clic sull'icona **Esporta come CSV** ().

  Nota: Per i timestamp nel log esportato viene utilizzata l'ora locale specificata dal browser Web.
- Escludere eventi di controllo specifici da tutte le pagine in cui vengono visualizzati gli eventi (vedere Esclusione di eventi).
- Restringere l'elenco degli eventi di controllo visualizzati nella pagina corrente:
  - Mostrare o nascondere gli eventi di una gravità specifica facendo clic sulle seguenti icone:
    - Icona **Eventi critici** ()
    - Icona **Eventi di avvertenza** ()
    - Icona **Eventi informativi** ()
  - Mostrare solo gli eventi con una data e un'ora specifiche. È possibile scegliere una delle seguenti opzioni dall'elenco a discesa:
    - Tutte le date
    - 2 ore precedenti
    - 24 ore precedenti
    - Scorsa settimana
    - Scorso mese
    - Custom

    Se si seleziona **Personalizzato**, è possibile filtrare gli eventi di gestione e hardware generati tra una data di avvio personalizzata e la data corrente.
  - Elencare solo gli eventi che contengono testo specifico immesso nel campo **Filtro**.
  - Ordinare gli eventi per colonna facendo clic sull'intestazione di una colonna.

Risoluzione di un evento

Lenovo XClarity Administrator fornisce informazioni sulle azioni appropriate da eseguire per risolvere un evento.

Procedura

Per risolvere un evento, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Monitoraggio → Log eventi** per visualizzare la pagina Log.

Passo 2. Fare clic sulla scheda **Log eventi**.

Passo 3. Individuare l'evento nel log eventi.

Passo 4. Per visualizzare le informazioni sull'evento (incluse le azioni di ripristino e una spiegazione) e sul dispositivo che lo ha generato, fare clic sul collegamento nella colonna **Evento**.

Passo 5. Fare clic sulla scheda **Dettagli**.

Passo 6. Completare le azioni di ripristino nella scheda **Dettagli** per risolvere l'evento.

Nota: se la spiegazione e l'azione di ripristino per un evento non vengono visualizzate, visitare il Documentazione online di Lenovo Flex System e cercare il titolo dell'evento. Nel sito Web sono sempre disponibili le informazioni più aggiornate.

Se, dopo essersi attenuti alla procedura consigliata, il problema persiste, contattare il Supporto Lenovo.

Esclusione di eventi

Se vengono visualizzati eventi che non interessano l'utente, è possibile escludere tali eventi da tutte le pagine in cui vengono visualizzati. Gli eventi esclusi compaiono ancora nel log ma vengono nascosti da tutte le pagine in cui sono visualizzati.

Informazioni su questa attività

Gli eventi esclusi vengono nascosti per tutti gli utenti, non solo per l'utente che imposta la configurazione.

È possibile impostare i dispositivi in modalità di manutenzione, in modo da escludere tutti gli eventi e gli avvisi relativi a questi dispositivi (vedere Impostazione dei dispositivi in modalità di manutenzione).

Restrizione: solo gli utenti con privilegi di amministratore possono escludere o ripristinare gli eventi.

Procedura

Per escludere gli eventi dal log eventi, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Monitoraggio → Log eventi**, quindi su **Log eventi**. Viene visualizzata la finestra di dialogo Log eventi.

Passo 2. Selezionare gli eventi da escludersi e fare clic sull'icona **Escludi eventi** ( ). Viene visualizzata la finestra di dialogo Escludi eventi.

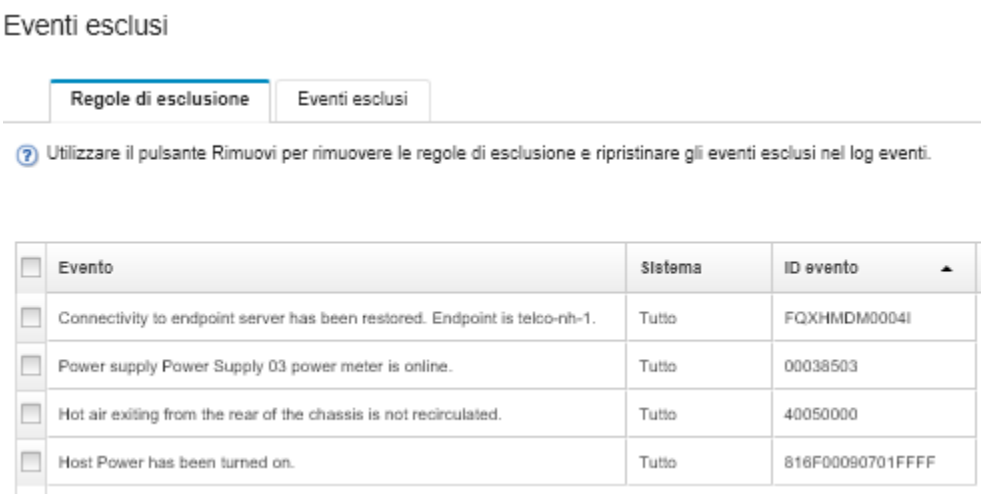
Passo 3. Selezionare una delle seguenti opzioni:
- **Escludi eventi selezionati da tutti i sistemi**. Esclude gli eventi selezionati da tutti i dispositivi gestiti.
- **Escludi eventi solo dai sistemi nell'ambito dell'istanza selezionata**. Esclude gli eventi selezionati dai dispositivi gestiti a cui si applicano.

Passo 4. Fare clic su **Salva**.

Al termine

Quando si escludono gli eventi, Lenovo XClarity Administrator crea regole di esclusione in base alle informazioni fornite.

- Visualizza un elenco di regole di esclusione e di eventi esclusi dalla pagina Log facendo clic sull'icona **Mostra eventi esclusi** ( ). Nella finestra di dialogo Eventi esclusi, fare clic sulla scheda **Regole di esclusione** per visualizzare le regole di esclusione oppure sulla scheda **Eventi esclusi** per visualizzare gli eventi esclusi.



- Ripristina gli eventi esclusi nel log eventi rimuovendo la regola di esclusione appropriata. Per rimuovere una regola di esclusione, fare clic sull'icona **Mostra eventi esclusi** icon ( ) per visualizzare la finestra di dialogo Eventi esclusi, selezionare le regole di esclusione da ripristinare, quindi fare clic su **Rimuovi esclusioni**.
- Prevenire che gli eventi che richiedono assistenza presenti nell'elenco degli eventi esclusi aprano automaticamente i report dei problemi, facendo clic su **Amministrazione → Assistenza e supporto** dalla barra dei menu di Lenovo XClarity Administrator, facendo clic sulla scheda **Server d'inoltro di servizio** e quindi selezionando **No** accanto alla domanda **Si desidera che gli eventi esclusi aprano i report dei problemi?**.

Inoltro di eventi

È possibile configurare Lenovo XClarity Administrator affinché inoltri gli eventi ai dispositivi mobili e alle applicazioni collegate nel proprio ambiente per aggregare e monitorare lo stato dell'hardware e i problemi di runtime per l'ambiente hardware.

Ulteriori informazioni: XClarity Administrator: monitoraggio

Inoltro di eventi a syslog, a un programma di gestione SNMP remoto e ad altri servizi di eventi

È possibile configurare Lenovo XClarity Administrator affinché inoltri gli eventi alle applicazioni collegate nel proprio ambiente per aggregare e monitorare lo stato dell'hardware e i problemi di runtime per l'ambiente hardware. È possibile definire l'ambito degli eventi da inoltrare in base al dispositivo, alla classe dell'evento, alla gravità dell'evento e al componente.

Informazioni su questa attività

Lenovo XClarity Administrator può inoltrare gli eventi per uno o più dispositivi. Per gli eventi di controllo, è possibile scegliere di inoltrare tutti gli eventi di controllo o nessuno. Non è possibile inoltrare eventi di controllo specifici. Per gli eventi di gestione e hardware, è possibile scegliere di inoltrare gli eventi per una o più gravità (eventi critici, di avvertenza e informativi) e per uno o più componenti (unità disco, processori e adattatori).

Lenovo XClarity Administrator utilizza i server d'inoltro degli eventi per inoltrare gli eventi. Un *server d'inoltro degli eventi* include le informazioni sul protocollo da utilizzare, sul destinatario, sui dispositivi da monitorare e sugli eventi da inoltrare. Dopo aver creato e abilitato un server d'inoltro degli eventi, Lenovo XClarity Administrator avvia il monitoraggio per gli eventi in entrata in base ai criteri del filtro. Quando viene rilevata una corrispondenza, per inoltrare l'evento viene utilizzato il protocollo associato.

Sono supportati i seguenti protocolli:

- **Azure Log Analytics**. Lenovo XClarity Administrator inoltra gli eventi monitorati in rete a Microsoft Azure Log Analytics.
- **E-mail**. Lenovo XClarity Administrator inoltra gli eventi monitorati ad uno o più indirizzi e-mail mediante SMTP. L'e-mail contiene informazioni sull'evento, il nome host del dispositivo sorgente e i collegamenti all'interfaccia Web di Lenovo XClarity Administrator e all'app Lenovo XClarity Mobile.
- **FTP**. Inoltra gli eventi monitorati in rete a un server FTP.
- **REST**. Lenovo XClarity Administrator inoltra gli eventi monitorati in rete a un Web Service REST.
- **SNMP**. Lenovo XClarity Administrator inoltra gli eventi monitorati sulla rete ad un programma di gestione SNMP remoto. I trap SNMPv1 e SNMPv3 sono supportati.

  Per informazioni sul file MIB (Management Information Base) che descrive i trap SNMP generati da Lenovo XClarity Administrator, vedere lenovoMgrAlert.mib filefile lenovoMgrAlert.mib nella documentazione online di Lenovo XClarity Administrator.
- **Syslog**. Lenovo XClarity Administrator inoltra gli eventi monitorati sulla rete a un server log centrale in cui gli strumenti nativi possono essere utilizzati per monitorare il syslog.

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Nota: Gli eventi non vengono recapitati se, ad esempio, la connettività tra Lenovo XClarity Administrator e il server d'inoltro degli eventi è interrotta o se la porta è bloccata.

Configurazione dell'inoltro eventi a Azure Log Analytics

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a Azure Log Analytics.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per Azure Log Analytics.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **Azure Log Analytics** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il nome e la descrizione facoltativa per il server d'inoltro degli eventi.
- Immettere la chiave primaria per l'interfaccia Azure Log Analytics.
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- **Facoltativo**: se è richiesta l'autenticazione, selezionare uno dei seguenti tipi di autenticazione:
  - **Base**. Esegue l'autenticazione server specificato utilizzando l'ID utente e la password specificati.
  - **Nessuna**. Non viene utilizzata nessuna autenticazione.

Passo 5. Fare clic su **Formato di output** per scegliere il formato di output dei dati dell'evento da inoltrare. Le informazioni variano per ciascun tipo di server d'inoltro degli eventi.

Il seguente formato di output di esempio è il formato predefinito per i destinatari Azure Log Analytics. Tutte le parole tra parentesi quadre doppie sono le variabili che vengono sostituite con i valori effettivi quando viene inoltrato un evento. Le variabili disponibili per i destinatari Azure Log Analytics sono elencate nella finestra di dialogo Formato di output.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
\"LXCA\":\"[[LXCA_IP]]\"}
```

È possibile fare clic su **Ripristina valori predefiniti** per modificare il formato di output e reimpostarlo in base ai campi predefiniti.

Passo 6. Fare clic sull'interruttore **Consenti eventi esclusi** per consentire o bloccare l'inoltro di un evento escluso.

Passo 7. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 8. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 9. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un

dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 10. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 11. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Corrispondenza per categoria eventi**.
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.
  4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
  6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I,FQXHMEM0214I`).
- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
  4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
  6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.
- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 12. Scegliere se includere determinati tipi di eventi.

- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi.
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 13. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 14. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 15. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 16. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

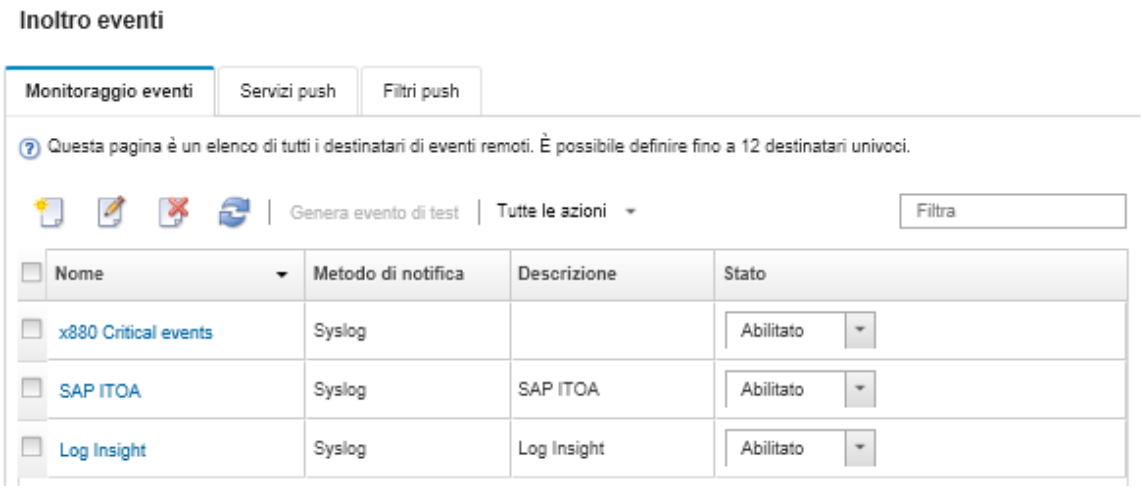
Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

1. Utilizzare le icone **Scorri a sinistra** (◀) e **Scorri a destra** (▶) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.
3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 17. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 18. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al server Azure Log Analytics appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.

- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ().
- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).

Configurazione dell'inoltro degli eventi a un servizio di posta elettronica mediante il protocollo SMTP

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a un servizio di posta elettronica utilizzando il protocollo SMTP.

Prima di iniziare

Per inoltrare l'e-mail a un servizio e-mail basato sul Web (ad esempio Gmail, Hotmail o Yahoo), il server SMTP deve supportare l'inoltro della posta elettronica Web.

Prima di configurare un server di inoltro degli eventi su un servizio Web di Gmail consultare le informazioni in Configurazione dell'inoltro eventi a un server SMTP GmailConfigurazione dell'inoltro eventi a syslog, a un programma di gestione SNMP remoto o a un'e-mail nella documentazione online di Lenovo XClarity Administrator.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per la posta elettronica mediante SMTP.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** (). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **E-mail** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il nome, la destinazione host e la descrizione facoltativa per il server d'inoltro degli eventi.
- Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è `25`.
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- Immettere l'indirizzo e-mail per ciascun destinatario. Separare gli indirizzi e-mail con una virgola.

Per inviare e-mail al contatto del supporto assegnato per il dispositivo, selezionare **Usa e-mail contatto del supporto** (vedere Definizione dei contatti di supporto per un dispositivo nella documentazione online di XClarity Administrator).

- **Facoltativo:** immettere l'indirizzo e-mail del mittente dell'e-mail (ad esempio, `john@company.com`).

  Se non viene specificato un indirizzo e-mail, l'indirizzo del mittente è `LXCA.`*<source_identifier>*`@`*<smtp_host>* per impostazione predefinita.

  Se viene specificato solo il dominio del mittente, il formato dell'indirizzo del mittente è *<LXCA_host_name>*@*<sender_domain>* (ad esempio, XClarity1@company.com).

  Note:

  - Se si configura un server SMTP affinché richieda un nome host per l'inoltro delle e-mail e non si configura un nome host per XClarity Administrator, è possibile che il server SMTP rifiuti gli eventi inoltrati. Se XClarity Administrator non dispone di un nome host, l'evento viene inoltrato con l'indirizzo IP. Se l'indirizzo IP non può essere ottenuto, verrà inviato "localhost". Ciò potrebbe far sì che il server SMTP rifiuti l'evento.
  - Se viene specificato il dominio del mittente, la fonte non si identifica nell'indirizzo del mittente. Vengono, invece, incluse le informazioni sulla fonte dell'evento nel corpo dell'e-mail, tra cui il nome di sistema, l'indirizzo IP, il tipo o il modello e il numero di serie.
  - Se il server SMTP accetta solo le e-mail inviate da un utente registrato, l'indirizzo predefinito del mittente (`LXCA.`*<source_identifier>*`@`*<smtp_host>*) viene rifiutato. In questo caso, è necessario specificare almeno un nome di dominio nel campo **Indirizzo di provenienza**.

- **Facoltativo:** per stabilire una connessione protetta al server SMTP, selezionare i seguenti tipi di connessione:
  - **SSL**. Utilizzare il protocollo SSL durante la comunicazione.
  - **STARTTLS**. Utilizzare il protocollo TLS per formare una comunicazione protetta su un canale non protetto.

  Se viene selezionato uno di questi tipi di connessione, LXCA tenta di scaricare e importare il certificato del server SMTP nel proprio archivio attendibile. All'utente verrà richiesto di accettare l'aggiunta di questo certificato nell'archivio attendibile.

- **Facoltativo:** se è richiesta l'autenticazione, selezionare uno dei seguenti tipi di autenticazione:
  - **Regolare**. Esegue l'autenticazione server SMTP specificato utilizzando l'ID utente e la password specificati.
  - **NTLM**. Utilizza il protocollo NT LAN Manager (NTLM) per eseguire l'autenticazione al server SMTP specificato utilizzando l'ID utente, la password e il nome di dominio specificati.
  - **OAUTH2**. Utilizza il protocollo Simple Authentication and Security Layer (SASL) per eseguire l'autenticazione al server SMTP specificato utilizzando il nome utente e il token di sicurezza specificati. Generalmente, il nome utente è l'indirizzo e-mail.

    Attenzione: il token di sicurezza scade dopo un breve periodo di tempo. L'aggiornamento del token di sicurezza è responsabilità dell'utente.
  - **Nessuna**. Non viene utilizzata nessuna autenticazione.

Passo 5. Fare clic su **Formato di output** per scegliere il formato di output dei dati dell'evento da inoltrare nel corpo dell'e-mail e il formato dell'oggetto dell'e-mail. Le informazioni variano per ciascun tipo di server d'inoltro degli eventi.

Il seguente formato di output di esempio è il formato predefinito per i destinatari dell'e-mail. Tutte le parole tra parentesi quadre doppie sono le variabili che vengono sostituite con i valori effettivi quando viene inoltrato un evento. Le variabili disponibili per i destinatari dell'e-mail sono elencate nella finestra di dialogo Formato output.

Oggetto dell'e-mail

```
[[DeviceName]]-[[EventMessage]]
```

Corpo dell'e-mail

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n
```

È possibile fare clic su **Ripristina valori predefiniti** per modificare il formato di output e reimpostarlo in base ai campi predefiniti.

Passo 6. Fare clic sull'interruttore **Consenti eventi esclusi** per consentire o bloccare l'inoltro di un evento escluso.

Passo 7. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 8. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 9. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 10. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 11. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Corrispondenza per categoria eventi**.
    1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
    2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
    3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.
    4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
    5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
    6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
    1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
    2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
    3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
    4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
    5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
    6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.
- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 12. Scegliere se includere determinati tipi di eventi.

- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi.
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 13. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 14. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 15. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 16. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

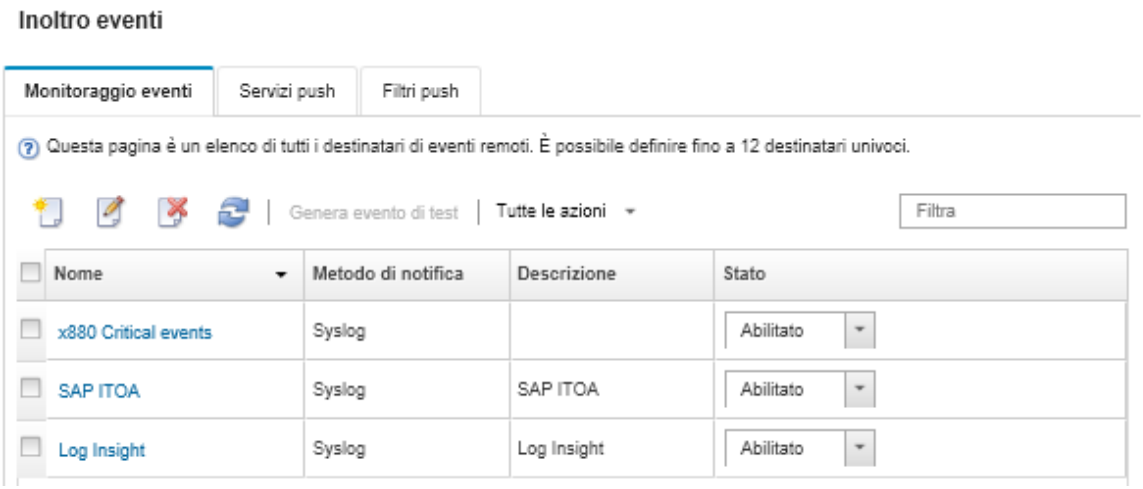
1. Utilizzare le icone **Scorri a sinistra** (◀) e **Scorri a destra** (▶) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.

3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 17. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 18. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al servizio di posta elettronica appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ( ).

- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).

Configurazione dell'inoltro eventi a un servizio SMTP Gmail

É possibile configurare Lenovo XClarity Administrator affinché inoltri eventi monitorati a un servizio e-mail basato su Web, come ad esempio Gmail.

Utilizzare i seguenti esempi di configurazione per impostare il server d'inoltro degli eventi affinché utilizzi il servizio SMTP di Gmail.

Nota: Gmail consiglia di utilizzare il metodo di autenticazione OAUTH2 per comunicazioni più sicure. Se si sceglie di utilizzare l'autenticazione regolare, verrà inviata un'e-mail per indicare che un'applicazione ha tentato di utilizzare l'account senza gli standard di sicurezza più recenti. Il messaggio include le istruzioni per la configurazione dell'account e-mail affinché accetti questi tipi di applicazioni.

Per informazioni sulla configurazione di un server SMTP di Gmail, vedere https://support.google.com/a/answer/176600?hl=en.

Autenticazione regolare mediante SSL sulla porta 465

Questo esempio comunica con il server SMTP di Gmail tramite il protocollo SSL sulla porta 465 ed esegue l'autenticazione mediante un account utente e una password Gmail validi.

Parametro	Valore
Host	smtp.gmail.com
Porta	465
SSL	Seleziona
STARTTLS	Cancella
Autenticazione	Regolare
Utente	Indirizzo e-mail Gmail valido
Password	Password di autenticazione Gmail
Indirizzo di provenienza	(facoltativo)

Autenticazione regolare mediante TLS sulla porta 587

Questo esempio comunica con il server SMTP di Gmail tramite il protocollo TLS sulla porta 587 ed esegue l'autenticazione mediante un account utente e una password Gmail validi.

Parametro	Valore
Host	smtp.gmail.com
Porta	587
SSL	Cancella
STARTTLS	Seleziona
Autenticazione	Regolare
Utente	Indirizzo e-mail Gmail valido
Password	Password di autenticazione Gmail
Indirizzo di provenienza	(facoltativo)

Autenticazione OAUTH2 mediante TLS sulla porta 587

Questo esempio comunica con il server SMTP di Gmail tramite il protocollo TLS sulla porta 587 ed esegue l'autenticazione mediante un account utente e un token di sicurezza Gmail validi.

Utilizzare la seguente procedura di esempio per ottenere il token di sicurezza.

1. Creare un progetto in Google Developers Console e recuperare l'ID e il client secret. Per ulteriori informazioni, visitare il sito Web Pagina Web per l'accesso di Google ai siti Web.
   a. Da un browser Web, aprire la Pagina Web delle API Google.
   b. Dal menu di quella pagina Web, fare clic su **Seleziona un progetto → Crea progetto**. Viene visualizzata la finestra di dialogo Nuovo progetto.
   c. Immettere un nome, selezionare **Sì** per accettare l'accordo di licenza e fare clic su **Crea**.
   d. Nella scheda **Panoramica**, utilizzare il campo di ricerca per cercare "gmail".
   e. Fare clic su **GMAIL API** nei risultati della ricerca.
   f. Fare clic su **Abilita**.
   g. Fare clic sulla scheda **Credenziali**.
   h. Fare clic su **Schermata consenso OAuth**.
   i. Immettere un nome nel campo **Nome del prodotto visualizzato dagli utenti** e fare clic su **Salva**.
   j. Fare clic su **Crea credenziali → ID client OAuth**.
   k. Selezionare **Altro** e immettere un nome.
   l. Fare clic su **Crea**. Viene visualizzata la finestra di dialogo Client OAuth con l'ID e il segreto client.
   m. Prendere nota dell'ID e del segreto client per utilizzarli in futuro.
   n. Fare clic su **OK** per chiudere la finestra di dialogo.
2. Utilizzare lo script Phyton oauth2.py per generare e autorizzare un token di sicurezza fornendo l'ID e il segreto client generato al momento della creazione del progetto.

   Nota: per completare questa operazione è necessario Python versione 2.7. È possibile scaricare ed installare Python 2.7 dal Sito Web di Python.
   a. Da un browser Web, aprire la Pagina Web gmail-oauth2-tools.
   b. Fare clic su **Non elaborato** e salvare il contenuto in un file denominato `oauth2.py` sul sistema locale.
   c. Eseguire il seguente comando come terminale (Linux) o come riga di comando (Windows):
      ```
      py oauth2.py --user=<your_email> --client_id=<client_id>
         --client_secret=<client_secret> --generate_oauth2_token
      ```
      Ad esempio
      ```
      py oauth2.py --user=jon@gmail.com
         --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
         --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
      ```
      Questo comando restituisce un URL da utilizzare per autorizzare il token e per recuperare un codice di verifica dal sito Web di Google, ad esempio:
      ```
      To authorize token, visit this url and follow the directions:

      https://accounts.google.com/o/oauth2/auth?client_id=884243132302
      -458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
      urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;scope=https%3A%2F%2Fmail.
      google.com%2F

      Enter verification code:
      ```
   d. Da un browser Web, aprire l'URL che è stato restituito nel passaggio precedente.

e. Fare clic su **Consenti** per accettare questo servizio. Viene restituito un codice di verifica.

f. Immettere il codice di verifica nel comando `oauth2.py`.

Il comando restituisce il token di sicurezza e aggiorna il token, ad esempio:

```
Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
Access Token Expiration Seconds: 3600
```

Importante: il token di sicurezza scade dopo un periodo di tempo. È possibile utilizzare lo script Phyton oauth2.py e il token di aggiornamento per generare un nuovo token di sicurezza. La generazione del nuovo token di sicurezza e l'aggiornamento del server di inoltro degli eventi tramite il nuovo token in Lenovo XClarity Administrator è responsabilità dell'utente.

3. Dall'interfaccia Web di Lenovo XClarity Administrator, configurare il server di inoltro degli eventi per e-mail utilizzando i seguenti attributi:

Parametro	Valore
Host	smtp.gmail.com
Porta	587
SSL	Cancella
STARTTLS	Seleziona
Autenticazione	OAUTH2
Utente	Indirizzo e-mail Gmail valido
Token	Token di sicurezza
Indirizzo di provenienza	(facoltativo)

Configurazione dell'inoltro di eventi a un server FTP

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a un server FTP.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per un server FTP.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **FTP** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il nome, la destinazione host e la descrizione facoltativa per i server d'inoltro degli eventi.
- Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è 21.
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- **Facoltativo:** specificare la sequenza di caratteri da rimuovere dal contenuto del file.
- Immettere il formato del nome file da utilizzare per il file che contiene l'evento inoltrato. Il formato predefinito è `event_[[EventSequenceID]].txt`.

  Nota: Ogni file contiene le informazioni per un singolo evento.
- Immettere il percorso del server FTP remoto su cui il file deve essere caricato.
- Scegliere la codifica dei caratteri: **UTF 8** o **Big5**. L'impostazione predefinita è UTF-8.
- Selezionare il tipo di autenticazione. É possibile selezionare uno dei seguenti valori.
  - **Anonimo**. (predefinito) Non viene utilizzata alcuna autenticazione
  - **Base**. Esegue l'autenticazione sul server FTP utilizzando l'ID utente e la password specificati.

Passo 5. Fare clic su **Formato di output** per scegliere il formato di output dei dati dell'evento da inoltrare. Le informazioni variano per ciascun tipo di server d'inoltro degli eventi.

Il seguente formato di output di esempio è il formato predefinito per i destinatari FTP. Tutte le parole tra parentesi quadre doppie sono le variabili che vengono sostituite con i valori effettivi quando viene inoltrato un evento. Le variabili disponibili per i destinatari FTP sono elencate nella finestra di dialogo Formato output.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
```

```
iOS link         : [[iOSLink]]\n
Android link     : [[AndroidLink]]\n
System Name      : [[DeviceFullPathName]]\n"
```

È possibile fare clic su **Ripristina valori predefiniti** per modificare il formato di output e reimpostarlo in base ai campi predefiniti.

Passo 6. Fare clic sull'interruttore **Consenti eventi esclusi** per consentire o bloccare l'inoltro di un evento escluso.

Passo 7. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 8. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 9. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 10. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 11. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Corrispondenza per categoria eventi**.
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.
  4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
  6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
  4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
  6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.

- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 12. Scegliere se includere determinati tipi di eventi.

- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi.
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 13. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 14. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 15. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 16. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

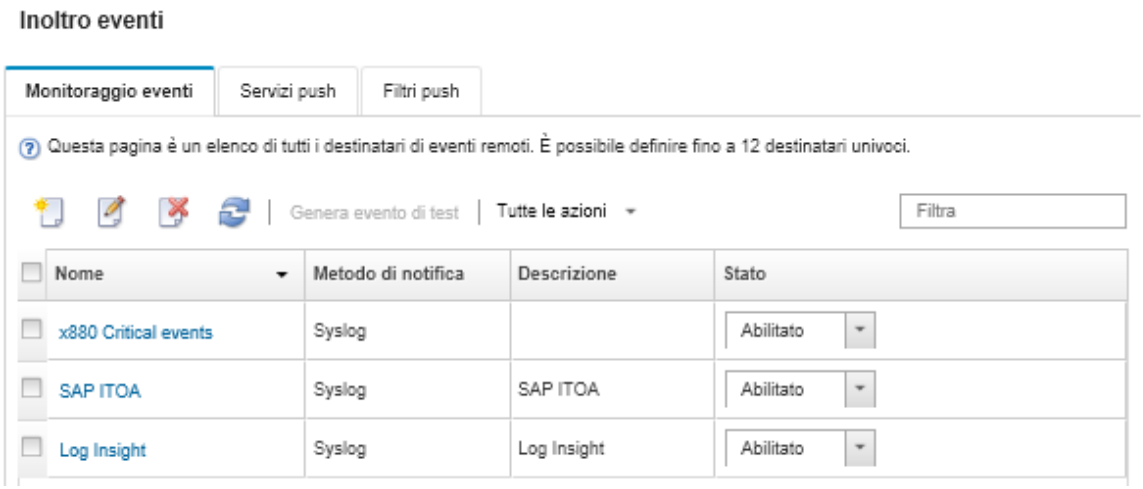
Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

1. Utilizzare le icone **Scorri a sinistra** (◄) e **Scorri a destra** (►) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.
3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 17. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 18. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al server FTP appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ( ).
- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).

Configurazione dell'inoltro eventi a un servizio Web REST

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a un servizio Web REST.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per un servizio Web REST.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **REST** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il percorso della risorsa in cui il server d'inoltro pubblicherà gli eventi (ad esempio, /rest/test).
- Selezionare il protocollo da utilizzare per l'inoltro di eventi. É possibile selezionare uno dei seguenti valori.
  - **HTTP**
  - **HTTPS**
- Selezionare il metodo REST. É possibile selezionare uno dei seguenti valori.
  - **PUT**
  - **POST**
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- **Facoltativo:** se è richiesta l'autenticazione, selezionare uno dei seguenti tipi di autenticazione:
  - **Base**. Esegue l'autenticazione server specificato utilizzando l'ID utente e la password specificati.
  - **Nessuna**. Non viene utilizzata nessuna autenticazione.

Passo 5. Fare clic su **Formato di output** per scegliere il formato di output dei dati dell'evento da inoltrare. Le informazioni variano per ciascun tipo di server d'inoltro degli eventi.

Il seguente formato di output di esempio è il formato predefinito per i destinatari del servizio Web REST. Tutte le parole tra parentesi quadre doppie sono le variabili che vengono sostituite con i valori effettivi quando viene inoltrato un evento. Le variabili disponibili per i destinatari del servizio Web REST sono elencate nella finestra di dialogo Formato output.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

È possibile fare clic su **Ripristina valori predefiniti** per modificare il formato di output e reimpostarlo in base ai campi predefiniti.

Passo 6. Fare clic sull'interruttore **Consenti eventi esclusi** per consentire o bloccare l'inoltro di un evento escluso.

Passo 7. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 8. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 9. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 10. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 11. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Corrispondenza per categoria eventi**.
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.
  4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
  6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
  4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
  6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.
- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 12. Scegliere se includere determinati tipi di eventi.

- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi.
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 13. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 14. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 15. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 16. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

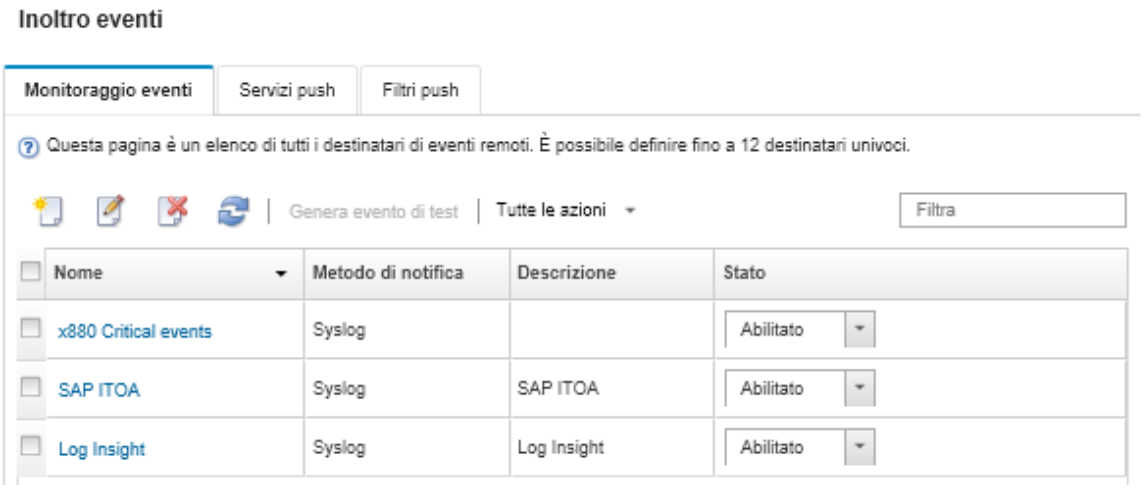
Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

1. Utilizzare le icone **Scorri a sinistra** (◀) e **Scorri a destra** (▶) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.
3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 17. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 18. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al servizio Web REST appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ().
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ().
- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).

Configurazione dell'inoltro eventi a un gestore SNMPv1 o SNMPv3 remoto

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a un gestore SNMPv1 o SNMPv3 remoto.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Per informazioni sull'utilizzo di MIB per XClarity Administrator, vedere file lenovoMgrAlert.mib.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per un gestore SNMPv1 o SNMPv3 remoto.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** (). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **SNMPv1** o **SNMPv3** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il nome e la destinazione host per il server d'inoltro degli eventi.
- Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è `162`.
- **Facoltativo:** immettere le informazioni aggiuntive, ad esempio la descrizione, il nome del contatto e la posizione.
- Selezionare la versione SNMP. É possibile selezionare uno dei seguenti valori.
  - **SNMPv1**. Se viene selezionata questa versione, specificare la password della comunità inviata con ogni richiesta SNMP al dispositivo.

– **SNMPv3**. Questa è la versione predefinita ed è consigliata per una protezione avanzata. Se è selezionata l'opzione SNMPv3, specificare, opzionalmente, l'ID utente, il tipo e la password di autenticazione e il tipo di privacy e la relativa password.

  Se il ricevitore trap SNMPv3 richiede l'ID del motore per l'istanza XClarity Administrator, è possibile individuare l'ID del motore eseguendo le seguenti operazioni:

  1. Verificare che i parametri della connessione (username, authProtocol, authPassword, privProtocol, privPassword) corrispondano a quelli configurati in XClarity Administrator.
  2. Utilizzando il software preferito (ad esempio snmpwalk), eseguire una richiesta GET SNMP sul server XClarity Administrator utilizzando uno dei seguenti OID:
     – EngineID: 1.3.6.1.6.3.10.2.1.1.0
     – EngineBoots : 1.3.6.1.6.3.10.2.1.2.0

     Utilizzare la seguente sintassi per eseguire questo comando `snmpget`. Il tipo di autenticazione del server d'inoltro -a può essere SHA o vuoto (nessuna autenticazione).
     ```
     snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDE
     ```

     Ad esempio, se l'indirizzo IP di XClarity Administrator è 192.0.1.0, il tipo di autenticazione è SHA e il tipo di privacy è AES, il comando che segue mostra l'ID del motore.
     ```
     snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_
     ```

     Viene restituita la seguente risposta di esempio. In questo esempio l'ID del motore è 0x80001370017F00000134C27E12.
     ```
     iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
     ```

- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- **Facoltativo**: se è necessaria l'autenticazione trap, immettere l'ID utente e la password di autenticazione. È necessario immettere lo stesso ID utente e password per il gestore SNMP remoto a cui sono stati inoltrati i trap.
- Selezionare il protocollo di autenticazione utilizzato dal gestore SNMP remoto per verificare il mittente del trap. É possibile selezionare uno dei seguenti valori
  – **SHA**. Utilizza il protocollo SHA per eseguire l'autenticazione al server SNMP specificato utilizzando l'ID utente, la password e il nome di dominio specificati.
  – **Nessuna**. Non viene utilizzata alcuna autenticazione
- Se è necessaria la crittografia del trap, immettere il tipo di privacy (protocollo di crittografia) e la password. É possibile selezionare uno dei seguenti valori. È necessario immettere lo stesso protocollo e password per il gestore SNMP remoto a cui sono stati inoltrati i trap.
  – **AES**
  – **DES**
  – **Nessuno**

Passo 5. Fare clic sull'interruttore **Consenti eventi esclusi** per consentire o bloccare l'inoltro di un evento escluso.

Passo 6. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 7. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 8. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un

dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 9. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 10. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Corrispondenza per categoria eventi**.
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.
  4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
  6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
  4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
  6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.
- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 11. Scegliere se includere determinati tipi di eventi.

- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.
- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi.
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 12. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 13. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 14. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 15. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

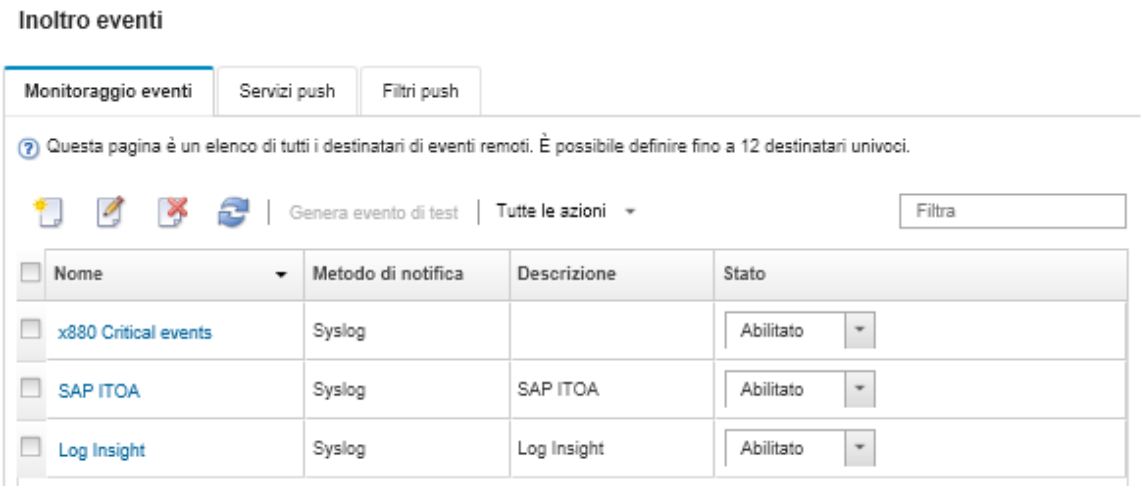
Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

1. Utilizzare le icone **Scorri a sinistra** (◀) e **Scorri a destra** (▶) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.
3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 16. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 17. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al gestore SNMP remoto appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.

- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ().
- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).
- Scaricare il file MIB contenente informazioni sui trap SNMP facendo clic sull'icona **Crea** (), quindi selezionando **Scarica file MIB** nella scheda Generale della finestra di dialogo Nuovo server d'inoltro eventi.

file lenovoMgrAlert.mib

Questo file MIB (Management Information Base) descrive i trap SNMP generati da Lenovo XClarity Administrator, inclusi gli avvisi generati da XClarity Administrator e dai dispositivi gestiti. È possibile compilare questo file MIB in qualsiasi programma di gestione SNMP in modo che i trap SNMP inviati da XClarity Administrator possano essere visualizzati significativamente.

È possibile scaricare il file MIB dall'interfaccia Web facendo clic su **Monitoraggio → Inoltro eventi** sulla barra dei menu, quindi sull'icona **Crea** (), selezionando **SNMP** per il tipo di server d'inoltro degli eventi e facendo clic su **Scarica file MIB** nella parte inferiore della finestra di dialogo.

I seguenti oggetti sono inclusi in tutti i trap SNMP in uscita. Gli oggetti aggiuntivi potrebbero essere inclusi in alcuni trap SNMP. Tutti gli oggetti sono descritti nel file MIB. Le informazioni di ripristino non sono incluse nel trap.

Nota: Questo elenco potrebbe differire da una versione di XClarity Administrator a un'altra.
- **mgrTrapAppId**. "Lenovo Event Manager".
- **mgrTrapCommonEvtID**. ID dell'evento comune
- **mgrTrapDateTime**. Data e ora locali in cui è stato generato l'evento
- **mgrTrapEventClass**. L'origine dell'evento. controllo, raffreddamento, alimentazione, dischi, memoria, processori, sistema, test, adattatore, espansione, modulo I/O o blade.
- **mgrTrapEvtID**. Identificativo univoco dell'evento
- **mgrTrapFailFRUs**. Elenco separato da virgola degli UUID FRU non validi, se applicabile
- **mgrTrapFailSNs**. Elenco separato da virgola dei numeri di serie per le FRU non valide, se applicabile.
- **mgrTrapFullyQualifiedDomainName**. Nome completo di dominio: il nome host e il nome di dominio.
- **mgrTrapID**. Trap ID
- **mgrTrapMsgText**. Testo del messaggio (solo inglese).
- **mgrTrapMsgID**. Identificativo del messaggio.
- **mgrTrapMtm**. Modello del tipo di modello del dispositivo che ha generato l'evento
- **mgrTrapService**. Indicatore dell'intervento richiesto: 000 (sconosciuto), 100 (nessuno), 200 (centro di assistenza) o 300 (cliente)
- **mgrTrapSeverity**. Indicatore della gravità: informativo, avvertenza, minore, principale o critico
- **mgrTrapSN**. Numero di serie del dispositivo che ha generato l'evento.
- **mgrTrapSrcIP**. Indirizzo IP del dispositivo da cui si è ricevuto l'evento.
- **mgrTrapSrcLoc**. Posizione del dispositivo che ha generato l'evento, solo in inglese (ad esempio, Slot xx)
- **mgrTrapSrcName**. Nome host o nome visualizzato del dispositivo che ha generato l'evento.
- **mgrTrapSysContact**. ID di contatto configurato dall'utente.
- **mgrTrapSysLocation**. Informazioni sulla posizione del dispositivo configurato dall'utente.
- **mgrTrapSystemName**. Nome del dispositivo, nome del componente e posizione dello slot.
- **mgrTrapTxtId**. Nome host o indirizzo IP del server Lenovo Event Manager che ha generato il trap.
- **mgrTrapUserid**. ID utente associato all'evento (se l'evento è interno e la classe dell'evento è Controllo)
- **mgrTrapUuid**. UUID del dispositivo che ha generato l'evento.

Configurazione dell'inoltro eventi a un syslog

È possibile configurare Lenovo XClarity Administrator in modo che inoltri eventi specifici a un syslog.

Informazioni su questa attività

È possibile creare e abilitare fino a 20 server d'inoltro degli eventi per inviare eventi a destinatari specifici.

Se XClarity Administrator viene riavviato dopo che i server d'inoltro degli eventi sono stati configurati, è necessario attendere che il server di gestione rigeneri i dati interni prima di inoltrare gli eventi correttamente.

Nota: Per XClarity Administrator v1.2.0 e versioni successive, l'opzione **Switch** è disponibile nella scheda **Eventi** nelle finestre di dialogo Nuovo server d'inoltro eventi e Modifica server d'inoltro eventi. Se è stato eseguito l'aggiornamento alla versione 1.2.0 o successive, ricordarsi di aggiornare i server d'inoltro degli eventi per includere o escludere gli eventi RackSwitch nel modo appropriato. Ciò è necessario anche quando si seleziona la casella di controllo **Tutti i sistemi** per selezionare tutti i dispositivi.

Procedura

Completare le seguenti operazioni per creare un server d'inoltro degli eventi per un syslog.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Server di inoltro degli eventi**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo server d'inoltro eventi.

Passo 4. Selezionare **syslog** come tipo di server d'inoltro degli eventi, quindi completare le informazioni specifiche del protocollo:

- Immettere il nome, la destinazione host e la descrizione facoltativa per il server d'inoltro degli eventi.
- Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è `514`.
- Selezionare il protocollo da utilizzare per l'inoltro di eventi. É possibile selezionare uno dei seguenti valori.
  - **UDP**
  - **TCP**
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- Facoltativamente, selezionare il formato data/ora del syslog. É possibile selezionare uno dei seguenti valori.
  - **Ora locale**. Il formato predefinito, ad esempio `Fri Mar 31 05:57:18 EDT 2017`.
  - **Ora GMT**. Standard internazionale (ISO8601) per la data e l'ora, ad esempio `2017-03-31T05:58:20-04:00`.

Passo 5. Fare clic su **Formato di output** per scegliere il formato di output dei dati dell'evento da inoltrare. Le informazioni variano per ciascun tipo di server d'inoltro degli eventi.

Il seguente formato di output di esempio è il formato predefinito per i destinatari sylog. Tutte le parole tra parentesi quadre doppie sono le variabili che vengono sostituite con i valori effettivi quando viene inoltrato un evento. Le variabili disponibili per i destinatari syslog sono elencate nella finestra di dialogo Formato output.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

È possibile fare clic su **Ripristina valori predefiniti** per modificare il formato di output e reimpostarlo in base ai campi predefiniti.

Passo 6. Fare clic sull'interruttore **Consenti eventi esclusi** per consentire o bloccare l'inoltro di un evento escluso.

Passo 7. Selezionare **Abilita questo server d'inoltro eventi** per attivare l'inoltro eventi per questo server d'inoltro eventi.

Passo 8. Fare clic su **Avanti** per visualizzare la scheda **Dispositivi**.

Passo 9. Selezionare i dispositivi e i gruppi che si desidera monitorare per questo server d'inoltro degli eventi.

Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.

Passo 10. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.

Passo 11. Selezionare i filtri da utilizzare per questo server d'inoltro degli eventi.

- **Corrispondenza per categoria eventi**.
  1. Per inoltrare tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Includi tutti gli eventi di controllo**.
  2. Per inoltrare tutti gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  3. Per inoltrare tutti gli eventi di modifica dello stato di integrità, selezionare **Includi eventi di modifica dello stato**.
  4. Per inoltrare tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Includi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da inoltrare.
  6. Immettere gli ID per uno o più eventi da escludere dall'inoltro. Separare gli ID con una virgola (ad esempio, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Corrispondenza per codice evento**. Immettere gli ID per uno o più eventi da inoltrare. Separare più ID con una virgola.
- **Escludi per categoria eventi**.
  1. Per escludere tutti gli eventi di controllo indipendentemente dal livello di stato, selezionare **Escludi tutti gli eventi di controllo**.
  2. Per escludere tutti gli eventi di garanzia, selezionare **Escludi eventi garanzia**.
  3. Per escludere tutti gli eventi di modifica dello stato di integrità, selezionare **Escludi eventi di modifica dello stato**.
  4. Per escludere tutti gli eventi di aggiornamento dello stato di integrità, selezionare **Escludi eventi di aggiornamento dello stato**.
  5. Selezionare le classi di evento e il livello di intervento richiesto da escludere.
  6. Immettere gli ID per uno o più eventi da inoltrare. Separare gli ID con una virgola.
- **Escludi per codice evento**. Immettere gli ID per uno o più eventi da escludere. Separare più ID con una virgola.

Passo 12. Scegliere se includere determinati tipi di eventi.

- **Includi tutti gli eventi di controllo**. Invia notifiche sugli eventi di controllo in base alle classi di evento e alle gravità selezionate.
- **Includi eventi garanzia**. Invia notifiche relative alle garanzie.

- **Includi eventi di modifica dello stato**. Invia notifiche relative alle modifiche dello stato.
- **Includi eventi di aggiornamento dello stato**. Notifiche inviate relative ai nuovi avvisi.
- **Includi eventi dei comunicati**. Invia una notifica sui nuovi comunicati.

Passo 13. Selezionare i tipi di eventi e le gravità per cui si desidera avvisati.

Passo 14. Scegliere se filtrare gli eventi in base all'intervento richiesto.

Passo 15. Fare clic su **Avanti** per visualizzare la scheda **Utilità di pianificazione**.

Passo 16. **Facoltativo:** definire le ore e i giorni in cui si desidera che gli eventi specificati vengano inoltrati a questo server d'inoltro degli eventi. Vengono inoltrati solo gli eventi che si verificano nell'intervallo di tempo specificato.

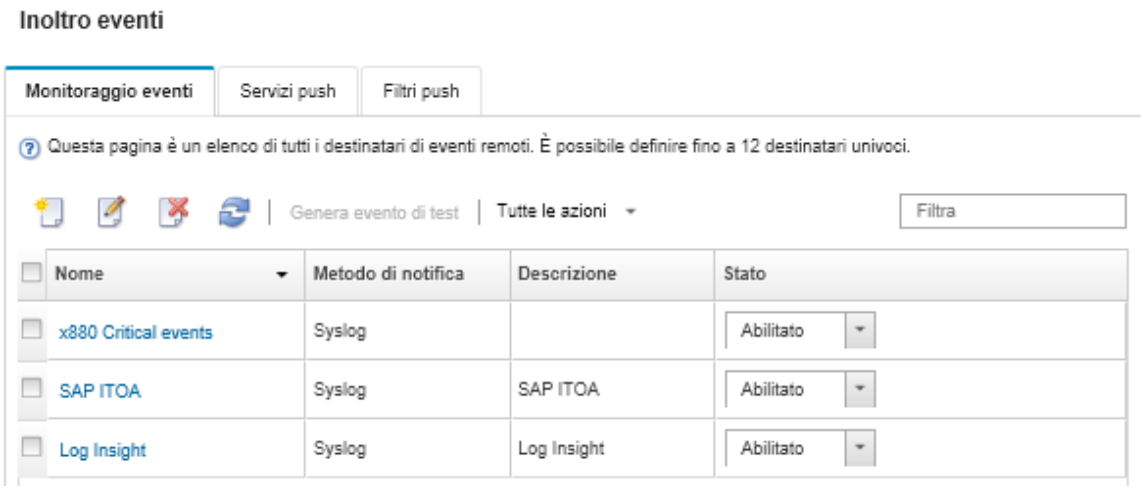
Se non viene creata una pianificazione per il server d'inoltro degli eventi, gli eventi vengono inoltrati 24 ore su 24, 7 giorni su 7.

1. Utilizzare le icone **Scorri a sinistra** (◀) e **Scorri a destra** (▶) e i pulsanti **Giorno**, **Settimana** e **Mese** per individuare il giorno e l'ora in cui si desidera avviare la pianificazione.
2. Fare doppio clic sull'intervallo di tempo per aprire la finestra di dialogo Nuovo periodo di tempo.
3. Fornire le informazioni richieste (la data, l'ora di avvio e di fine) e indicare se si desidera che la pianificazione venga ripetuta.
4. Fare clic su **Crea** per salvare la pianificazione e chiudere la finestra di dialogo. La nuova pianificazione verrà aggiunta al calendario.

Suggerimento:
- È possibile modificare l'intervallo di tempo trascinando la voce relativa alla pianificazione su un altro intervallo di tempo nel calendario.
- È possibile modificare la durata selezionando la parte superiore o inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare l'ora di fine selezionando la parte inferiore della voce relativa alla pianificazione e trascinandola sul nuovo orario del calendario.
- È possibile modificare una pianificazione facendo doppio clic sulla voce relativa alla pianificazione nel calendario e quindi facendo clic su **Modifica voce**.
- È possibile visualizzare un riepilogo di tutte le voci relative alla pianificazione selezionando **Mostra riepilogo utilità di pianificazione**. Il riepilogo include l'intervallo di tempo per ciascuna voce e le voci ripetibili.
- È possibile eliminare una voce relativa alla pianificazione dal calendario o dal riepilogo dell'utilità di pianificazione selezionando la voce e facendo clic su **Elimina voce**.

Passo 17. Fare clic su **Crea**.

Il server d'inoltro degli eventi viene elencato nella tabella Inoltro eventi.



Passo 18. Selezionare il nuovo server d'inoltro degli eventi, fare clic su **Genera evento di test** e verificare che gli eventi vengano correttamente inoltrati al syslog appropriato.

Al termine

Dalla pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un server d'inoltro degli eventi selezionato:

- Aggiornare l'elenco dei server d'inoltro degli eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un server d'inoltro degli eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del server d'inoltro degli eventi e i criteri del filtro, facendo clic sul nome del server d'inoltro degli eventi nella colonna **Nome**.
- Eliminare il server d'inoltro degli eventi facendo clic sull'icona **Elimina** ( ).
- Sospendere l'inoltro eventi (vedere Sospensione dell'inoltro eventi).

Sospensione dell'inoltro eventi

È possibile sospendere l'inoltro eventi disabilitando il server d'inoltro eventi. La sospensione dell'inoltro eventi interrompe il monitoraggio degli eventi in entrata. Gli eventi ricevuti al momento della sospensione del monitoraggio non vengono inoltrati.

Informazioni su questa attività

Lo stato Disabilitato non è permanente. Se il nodo di gestione viene riavviato, tutti i server d'inoltro degli eventi vengono abilitati.

Procedura

Attenersi alla procedura descritta di seguito per disabilitare l'inoltro di eventi.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Selezionare **Disabilita** nella colonna **Stato** per ciascun server d'inoltro degli eventi che si desidera sospendere.

Inoltro di eventi a dispositivi mobili

È possibile configurare Lenovo XClarity Administrator affinché esegua il push delle notifiche degli eventi ai dispositivi mobili

Prima di iniziare

Per inoltrare gli eventi ai dispositivi mobili devono essere soddisfatti i seguenti requisiti:

- Verificare che un server DNS valido sia configurato per consentire a Lenovo XClarity Administrator di collegarsi ai server push Apple o Google. Il server può essere configurato facendo clic su **Amministrazione → Accesso alla rete → Modifica accesso alla rete** , quindi facendo clic sulla scheda **Impostazioni Internet** (vedere Configurazione dell'accesso alla rete).
- Verificare che tutte le porte necessarie per la gestione degli eventi siano aperte sulla rete e sui firewall. Per informazioni sui requisiti delle porte, vedere Disponibilità della porta nella documentazione online di Lenovo XClarity Administrator.

Informazioni su questa attività

Quando l'app Lenovo XClarity Mobile è installata su un dispositivo mobile, è possibile abilitare ogni istanza collegata di Lenovo XClarity Administrator affinché esegua il push delle notifiche degli eventi al dispositivo mobile selezionato. Quando le notifiche push sono abilitate per un'istanza specifica, viene creata una sottoscrizione in Lenovo XClarity Administrator per il dispositivo mobile selezionata.

È possibile definire gli eventi di cui è stato eseguito il push nel dispositivo mobile assegnando filtri eventi globali predefiniti o personalizzati per ciascuna istanza di Lenovo XClarity Administrator. I filtri eventi globali sono abilitati per impostazione predefinita. Lenovo XClarity Administrator avvia il monitoraggio degli eventi in entrata in base ai criteri dei filtri. Quando viene rilevata una corrispondenza, l'evento viene inoltrato al dispositivo mobile.

Per ulteriori informazioni su Lenovo XClarity Mobile e sui dispositivi mobili supportati, vedere Utilizzo dell'app Lenovo XClarity Mobile.

Procedura

Per configurare le notifiche push sul dispositivo mobile selezionato, attenersi alla procedura descritta di seguito dall'app Lenovo XClarity Mobile sul dispositivo mobile.

Passo 1. Abilitare le notifiche push:

- È possibile abilitare le notifiche push quando si crea una connessione ad un'istanza Lenovo XClarity Administrator. Le notifiche push sono abilitate per impostazione predefinita.
- È possibile abilitare le notifiche push sulle connessioni esistenti abilitando uno o più filtri eventi

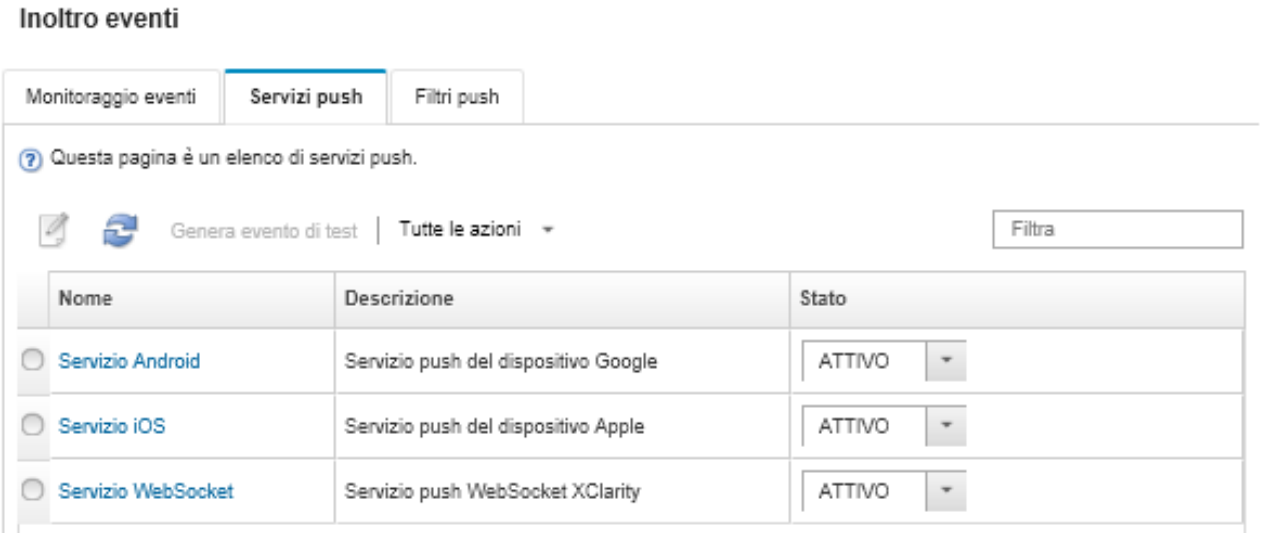
Passo 2. Assegnare i filtri eventi globali per specificare gli eventi che devono essere inoltrati al dispositivo mobile:

Nota: è possibile aggiungere o rimuovere i filtri eventi globali dalla sottoscrizione solo dall'app Lenovo XClarity Mobile. È possibile creare i filtri eventi globali solo dall'interfaccia Web Lenovo XClarity Administrator. Per informazioni sulla creazione di filtri eventi globali personalizzati, vedere Creazione di filtri eventi per dispositivi mobili e WebSockets.

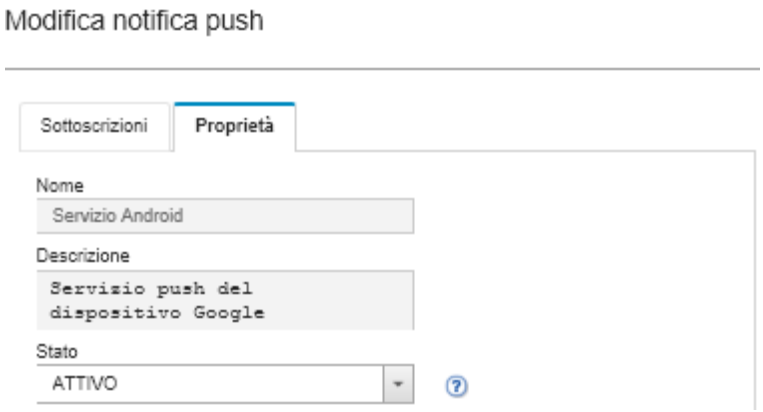
1. Toccare **Impostazioni → Notifiche push**. Viene visualizzato un elenco di connessioni Lenovo XClarity Administrator.
2. Toccare l'istanza Lenovo XClarity Administrator per visualizzare un elenco di filtri push.
3. Abilitare i filtri eventi per gli eventi di cui si desidera eseguire il push sul dispositivo mobile per l'istanza Lenovo XClarity Administrator.
4. Toccare **Tocca per generare notifica push di prova** per verificare che il push delle notifiche degli eventi venga eseguito correttamente.

Risultati

È possibile gestire le sottoscrizioni dalla pagina Inoltro eventi nell'interfaccia Web di Lenovo XClarity Administrator. Fare clic su **Monitoraggio → Inoltro eventi** per visualizzare la pagina Inoltro eventi.



- È possibile modificare le proprietà del servizio di notifica del dispositivo dalla scheda **Servizio push** nella pagina Inoltro eventi facendo clic sul collegamento relativo al servizio di notifica push (Google o Apple) nella colonna **Nome** per visualizzare la finestra di dialogo Modifica notifica push, quindi fare clic sulla scheda **Proprietà**.



- È possibile abilitare e disabilitare le sottoscrizioni:
  - Abilitare o disabilitare tutte le sottoscrizioni per un servizio di notifica di un dispositivo specifico dalla scheda **Servizio push** nella pagina Inoltro eventi selezionando lo stato **ATTIVATO** o **DISATTIVATO** nella tabella del servizio di notifica del dispositivo.
  - Abilitare o disabilitare tutte le sottoscrizioni per uno specifico dispositivo dall'app Lenovo XClarity Mobile toccando **Impostazioni → Notifica push**, quindi abilitando o disabilitando l'opzione Notifica push abilitata.
  - Abilitare o disabilitare una sottoscrizione specifica dall'app Lenovo XClarity Mobile toccando **Impostazioni → Notifica push**, toccando una connessione Lenovo XClarity Administrator e abilitando almeno un filtro eventi oppure disabilitando tutti i filtri eventi.
- È possibile generare un evento di prova per tutte le sottoscrizioni per uno specifico servizio mobile dalla scheda **Servizio push** nella pagina Inoltro eventi selezionando il servizio mobile e facendo clic su **Genera evento di test**.

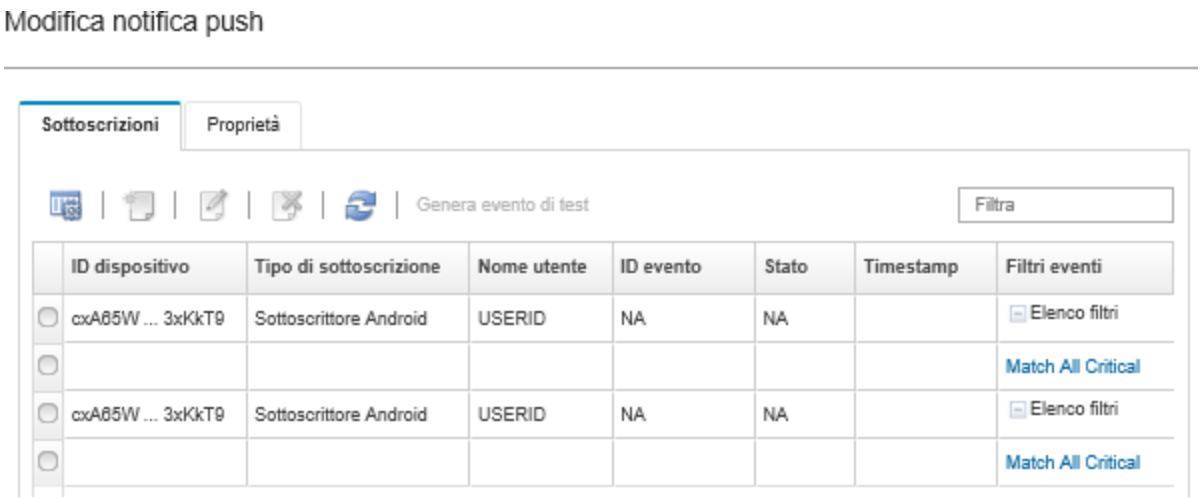
- È possibile visualizzare un elenco delle sottoscrizioni correnti. Dalla scheda **Servizio push** nella pagina Inoltro eventi, fare clic sul collegamento del servizio di notifica del dispositivo applicabile (Android o iOS) nella colonna **Nome** per visualizzare la finestra di dialogo Modifica notifica push, quindi fare clic sulla scheda **Sottoscrizioni**. L'ID del dispositivo identifica ciascuna sottoscrizione.

  Suggerimenti:

  – L'ID del dispositivo è costituito dalla prima cifra e dalle ultime 6 cifre dell'ID della registrazione push. L'ID della registrazione push può essere individuato dall'app Lenovo XClarity Mobile toccando **Impostazioni → Informazioni su → ID registrazione push**.

  – Se l'utente ha eseguito il login con uno dei seguenti ruoli vengono visualizzate tutte le sottoscrizioni; altrimenti vengono visualizzate solo le sottoscrizioni per l'utente che ha eseguito il login.
    – **lxc-admin**
    – **lxc-supervisor**
    – **lxc-security-admin**
    – **lxc-sysmgr**

- È possibile visualizzare l'elenco dei filtri eventi assegnati alla sottoscrizione dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push espandendo l'opzione **Elenco filtri** nella colonna **Filtri eventi** per la sottoscrizione.

- È possibile creare i filtri eventi per una sottoscrizione specifica dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push selezionando la sottoscrizione e facendo clic sull'icona **Crea** ( ).

  Nota: questi filtri eventi si applicano solo a una sottoscrizione specifica e non possono essere utilizzati da altre sottoscrizioni.

  È inoltre possibile modificare o rimuovere un filtro eventi selezionando il filtro eventi e facendo clic rispettivamente sull'icona **Modifica** ( ) o **Rimuovi** ( ).

- È possibile determinare lo stato dell'esecuzione del push più recente per una sottoscrizione specifica dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push. La colonna **Timestamp** indica la data e l'ora dell'ultimo push. L'opzione **Stato** indica se la notifica push è stata recapitata correttamente al servizio push. Non esiste nessuno stato indicante se la notifica push è stata correttamente recapitata dal servizio al dispositivo. Se il recapito di un servizio push non riesce, la colonna Stato fornisce informazioni aggiuntive relative all'errore.
- È possibile generare un evento di prova per una sottoscrizione specifica dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push selezionando la sottoscrizione e facendo clic su **Genera evento di test**.

- È possibile rimuovere una sottoscrizione dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push selezionando la sottoscrizione e facendo clic sull'icona **Rimuovi** ( ).

Inoltro di eventi ai servizi WebSocket

È possibile configurare Lenovo XClarity Administrator affinché esegua il push delle notifiche degli eventi ai servizi WebSocket.

Informazioni su questa attività

Le sottoscrizioni WebSocket non vengono memorizzate in modo permanente in Lenovo XClarity Administrator. Quando Lenovo XClarity Administrator viene riavviato, i sottoscrittori WebSocket devono eseguire nuovamente la registrazione.

Procedura

Per eseguire il push della notifica dell'evento a un servizio WebSocket, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.

Passo 2. Fare clic sulla scheda **Servizi push**.

Passo 3. Fare clic sul collegamento per il **servizio WebSocket** nella colonna **Nome**. Viene visualizzata la finestra di dialogo Modifica notifica push.

Passo 4. Fare clic sulla scheda **Sottoscrizioni**.

Passo 5. Fare clic sull'icona **Crea** ( ).

Passo 6. Immettere l'indirizzo IP dell'host di destinazione.

Passo 7. Fare clic su **Crea**.

Passo 8. Selezionare la nuova sottoscrizione, fare clic su **Genera evento di test**, quindi verificare che gli eventi siano inoltrati correttamente al servizio WebSocket.

Risultati

Dalla scheda **Sottoscrizioni** nella finestra di dialogo Modifica notifica push, è possibile eseguire le seguenti azioni su una sottoscrizione WebSocket selezionata:

- Aggiornare l'elenco dei servizi WebSocket facendo clic sull'icona **Aggiorna** ( ).
- Eliminare le sottoscrizioni selezionando le sottoscrizioni e facendo clic sull'icona **Elimina** ( ).
- Determinare lo stato dell'ultimo push tentato per una sottoscrizione specifica visualizzando il contenuto della colonna **Stato**. Se il tentativo non riesce, questa colonna contiene un messaggio che descrive l'errore.

Dalla scheda **Proprietà** nella finestra di dialogo Modifica notifica push, procedere come segue:

- Modificare le proprietà del servizio WebSocket, tra cui il tempo di inattività della connessione, le dimensioni massime del buffer, il numero massimo di sottoscrittori e il periodo di timeout del registro.
- È possibile ripristinare i valori predefiniti del servizio WebSocket facendo clic su **Ripristina valori predefiniti**.
- Sospendere l'esecuzione del push delle notifiche degli eventi a tutte le sottoscrizioni per il servizio WebSocket impostando l'opzione **Stato** su Disattivato.

Dalla scheda **Servizio push** nella pagina Inoltro eventi, è possibile generare un evento di prova per tutte le sottoscrizioni WebSocket selezionando il servizio WebSocket e facendo clic su **Genera evento di test**.

Creazione di filtri eventi per dispositivi mobili e WebSockets

È possibile creare filtri eventi globali da utilizzare in una o più sottoscrizioni per dispositivi mobili e WebSockets. È inoltre possibile creare filtri eventi univoci per una sottoscrizione.

Prima di iniziare

È necessario disporre dei privilegi di supervisore per creare i filtri eventi.

È possibile creare un massimo di 20 filtri eventi globali.

Informazioni su questa attività

Sono predefiniti i seguenti filtri eventi globali:

- **Associa tutti gli eventi Critico**. Questo filtro associa tutti gli eventi critici generati dal dispositivo gestito o da XClarity Administrator.
- **Associa tutti gli eventi Avvertenza**. Questo filtro associa tutti gli eventi di avvertenza generati dal dispositivo gestito o da XClarity Administrator.

Procedura

Per creare un filtro eventi globale, completare le seguenti operazioni.

- Creare un filtro eventi globale da utilizzare per ciascuna sottoscrizione.
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro eventi.
  2. Fare clic sulla scheda **Filtri push**.
  3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo filtro push.
  4. Specificare il nome e la descrizione dell'opzione per questo filtro eventi.
  5. Fare clic su **Avanti** per visualizzare la scheda **Sistemi**.
  6. Selezionare i dispositivi che si desidera monitorare.

     Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.
  7. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.
  8. Selezionare i componenti e le gravità per cui si desidera inoltrare gli eventi.

     Suggerimento:
     - Per inoltrare tutti gli eventi hardware, selezionare **Associa tutti gli eventi**.
     - Per inoltrare gli eventi di controllo, selezionare **Includi tutti gli eventi di controllo**.
     - Per inoltrare gli eventi di garanzia, selezionare **Includi eventi garanzia**.
  9. Fare clic su **Crea**.
- Creare un filtro eventi per una sottoscrizione specifica:
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitoraggio → Inoltro eventi**. Viene visualizzata la pagina Inoltro nuovi eventi.

2. Fare clic sulla scheda **Filtri push**.
3. Selezionare il collegamento per il tipo di dispositivo mobile (Android o iOS) nella colonna Nome della tabella. Viene visualizzata la finestra di dialogo Modifica notifica push.
4. Fare clic sulla scheda **Sottoscrizioni** per visualizzare un elenco di sottoscrizioni attive.
5. Selezionare la sottoscrizione e fare clic sull'icona **Crea** ( ). Viene visualizzata la scheda **Generale** della finestra di dialogo Nuovo filtro eventi.
6. Specificare il nome e la descrizione dell'opzione per questo filtro eventi.
7. Fare clic su **Avanti** per visualizzare la scheda **Sistemi**.
8. Selezionare i dispositivi che si desidera monitorare.

   Suggerimento: per inoltrare gli eventi per tutti i dispositivi gestiti (correnti e futuri), selezionare la casella di controllo **Associa tutti i sistemi**.Se non si seleziona la casella di controllo **Associa tutti i sistemi**, verificare che per i dispositivi selezionati non sia specificato DUMMY-UUID nella colonna UUID. Un UUID fittizio viene assegnato ai dispositivi che non sono stati ancora ripristinati dopo un riavvio o non sono stati completamente rilevati dal server di gestione. Se si seleziona un dispositivo con un UUID fittizio, l'inoltro eventi funziona per il dispositivo fino al momento in cui il dispositivo viene completamente rilevato o ripristinato e l'UUID fittizio diventa l'UUID reale.
9. Fare clic su **Avanti** per visualizzare la scheda **Eventi**.
10. Selezionare i componenti e le gravità per cui si desidera inoltrare gli eventi.

    Suggerimento:
    - Per inoltrare tutti gli eventi hardware, selezionare **Associa tutti gli eventi**.
    - Per inoltrare gli eventi di controllo, selezionare **Includi tutti gli eventi di controllo**.
    - Per inoltrare gli eventi di garanzia, selezionare **Includi eventi garanzia**.
11. Fare clic su **Crea**.

Al termine

Dalla scheda Filtri push nella pagina Inoltro eventi, è possibile eseguire le seguenti azioni su un filtro eventi selezionato:

- Aggiornare l'elenco dei filtri eventi facendo clic sull'icona **Aggiorna** ( ).
- Visualizzare i dettagli su un filtro eventi specifico facendo clic sul collegamento nella colonna **Nome**.
- Modificare le proprietà del filtro eventi e filtrare i criteri facendo clic sull'icona **Modifica** ( ).

Eliminare il filtro eventi facendo clic sull'icona **Elimina** ( ).

Utilizzo dei processi

I *processi* sono attività che richiedono tempi di esecuzione superiori per uno o più dispositivi. È possibile pianificare l'esecuzione di determinati processi per una sola volta (immediatamente o in secondo momento), in modo periodico o quando si verifica un evento specifico.

I processi vengono eseguiti in background. È possibile visualizzare lo stato di ciascun processo dal log dei processi.

Monitoraggio dei processi

È possibile visualizzare un log di tutti i processi avviati da Lenovo XClarity Administrator. Il log dei processi include i processi in esecuzione, completati o in errore.

Informazioni su questa attività

I *processi* sono attività che richiedono tempi di esecuzione superiori per uno o più dispositivi. Ad esempio, se un sistema operativo viene distribuito su più server, ciascuna distribuzione server viene elencata come processo separato.

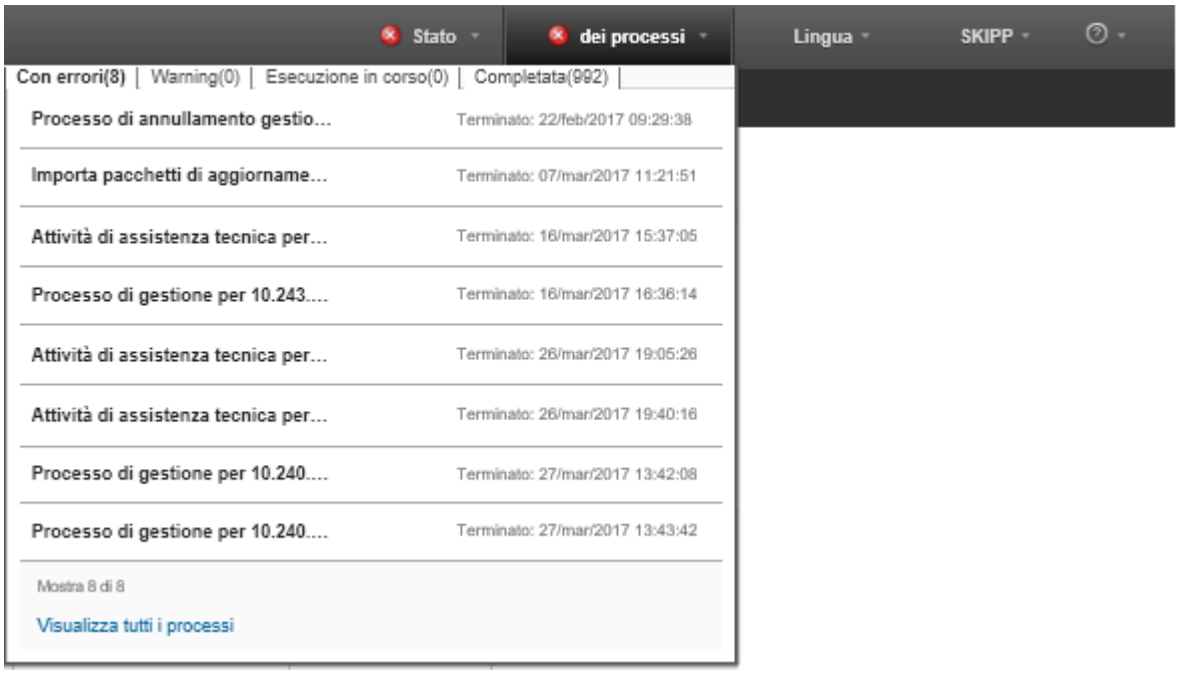
I processi vengono eseguiti in background. È possibile visualizzare lo stato di ciascun processo dal log dei processi.

Il log dei processi contiene informazioni su ciascun processo. Il log può contenere massimo 1.000 processi o 1 GB. Quando le dimensioni massime vengono raggiunte, i processi meno recenti completati correttamente vengono eliminati. Se nel log non sono presenti processi completati correttamente, vengono eliminati i processi meno recenti completati con avvisi. Se nel log non sono presenti processi completati correttamente o con avvisi, vengono eliminati i processi meno recenti completati con errori.

Procedura

Completare una delle seguenti operazioni per visualizzare il log processi.

- Dalla barra del titolo XClarity Administrator, fare clic su **Processi** per visualizzare un riepilogo dei processi in esecuzione, completati e in errore.



  Da questo menu a discesa è possibile fare clic sulle seguenti schede:
  - **Errori**. Visualizza un elenco di tutti i processi con errori associati.
  - **Avvisi**. Visualizza un elenco di tutti i processi con avvisi associati.
  - **Esecuzione in corso**. Visualizza un elenco di tutti i processi attualmente in esecuzione.
  - **Completato**. Visualizza un elenco di tutti i processi completati.

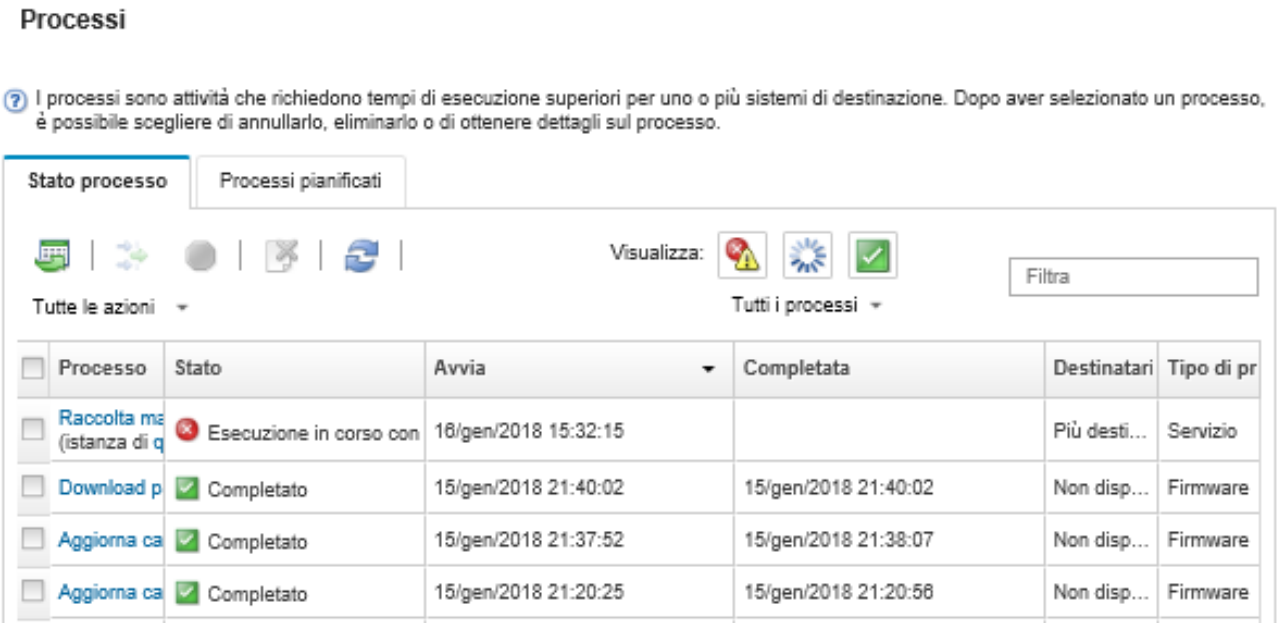
  Passare con il mouse sulla voce relativa a un processo nel menu a discesa per ulteriori informazioni relative al processo, quali lo stato, l'avanzamento e l'utente che ha creato il processo.

- Dalla barra del titolo di XClarity Administrator, fare clic su **Processi** e sul collegamento **Visualizza tutti i processi** per visualizzare la pagina Stato dei processi.

- Dalla barra dei menu di XClarity Administrator, fare clic su **Monitor → Processi** e sulla scheda **Stato dei processi** per visualizzare la pagina Stato dei processi.

Al termine

Viene visualizzata la pagina Processi con un elenco di tutti i processi per XClarity Administrator.



Da questa pagina, è possibile eseguire le seguenti azioni:

- Per creare pianificazioni dei processi, fare clic sulla scheda **Processi pianificati** (vedere Pianificazione dei processi).
- Visualizzare più informazioni su un processo, facendo clic sulla descrizione del processo nella colonna **Processi**. Viene visualizzata una finestra di dialogo con un elenco di attività secondarie (processi secondari) e le relative destinazioni, un riepilogo delle attività secondarie, incluse eventuali azioni necessarie e i dettagli del log, come la gravità e il timestamp per ogni messaggio. È possibile scegliere di visualizzare o nascondere i log per le attività secondarie.
- Per i processi pianificati, è possibile visualizzare le informazioni sulla pianificazione del processo facendo clic su "questo" collegamento, sotto la descrizione del processo nella colonna **Processi**.
- Modificare il numero di processi visualizzati per pagina. L'impostazione predefinita è 10 processi. È possibile visualizzare 25, 50 o tutti i processi.
- Restringere l'elenco dei processi visualizzati:
  - Per elencare solo i processi di una fonte specifica, fare clic su **Tipi di processo** e scegliere tra le seguenti opzioni.
    - **Tutti i tipi di processo**
    - **Service**
    - **Management**
    - **Configuration**
    - **Firmware**
    - **Health**
    - **Power**
    - **Accesso remoto**
    - **ID sistema**
    - **Immagini sistema operativo**

  - **Distribuzione sistema operativo**
  - **Esportazione profilo sistema operativo**
  - **Custom**
  - **Inventory**
  - **Sconosciuto**
- Per elencare solo i processi pianificati, associati a un tipo specifico di pianificazione, fare clic su **Tipi di pianificazione** e scegliere tra le seguenti opzioni.
  - **Tutti i tipi di pianificazione**
  - **Una volta**
  - **Periodico**
  - **Attivato**
- Nascondere o mostrare i processi con errori o avvertenze facendo clic sull'icona **Nascondi processi con errori/avvisi** ( ).
- Nascondere o mostrare i processi attualmente in esecuzione facendo clic sull'icona **Nascondi processi in esecuzione** ( ).
- Nascondere o mostrare i processi completati facendo clic sull'icona **Nascondi processi completati** ( ).
- Elencare solo i processi che contengono testo specifico immettendo il testo nel campo **Filtro**.
- Se il filtro viene applicato alla pagina, rimuovere il filtro facendo clic sull'icona **Mostra tutti i processi** ( ).
- Ordinare i processi per colonna facendo clic su un'intestazione di colonna.

- Esportare l'elenco dei processi come file CSV facendo clic sull'icona **Esporta come CSV** ( ).

  Nota: Per i timestamp nel log esportato viene utilizzata l'ora locale specificata dal browser Web.
- Annullare i processi o le sottoattività in esecuzione selezionando uno o più processi in esecuzione e facendo clic sull'icona **Interrompi** ( ).

  Nota: l'annullamento del processo potrebbe richiedere alcuni minuti.
- Eliminare i processi o le sottoattività completati dal log dei processi selezionando uno o più processi o sottoattività completati e facendo clic sull'icona **Elimina** ( ).
- Esportare le informazioni su processi specifici selezionando i processi e facendo clic sull'icona **Esporta come CSV** ( ).
- Aggiornare il log dei processi facendo clic sull'icona **Aggiorna** ( ).

Pianificazione dei processi

È possibile creare pianificazioni in Lenovo XClarity Administrator per eseguire determinate attività in momenti specifici.

Informazioni su questa attività

È possibile pianificare i seguenti tipi di processi:
- Attività semplici, come spegnimento e riavvio
- Raccolta dei dati di servizio per dispositivi specifici
- Aggiornamento dei cataloghi degli aggiornamenti firmware e dei driver di dispositivo del sistema operativo dal sito Web Lenovo

- Aggiornando XClarity Administrator viene aggiornato il catalogo dal sito Web Lenovo
- Download di firmware dal sito Web Lenovo
- Aggiornamento del firmware e dei driver di dispositivo del sistema operativo sui dispositivi gestiti
- Backup dei dati e delle impostazioni di XClarity Administrator
- Backup e ripristino dei dati di configurazione di uno switch

È possibile pianificare l'esecuzione dei processi:
- Una volta (immediatamente o in un secondo momento)
- Periodico
- Quando si verifica un evento specifico

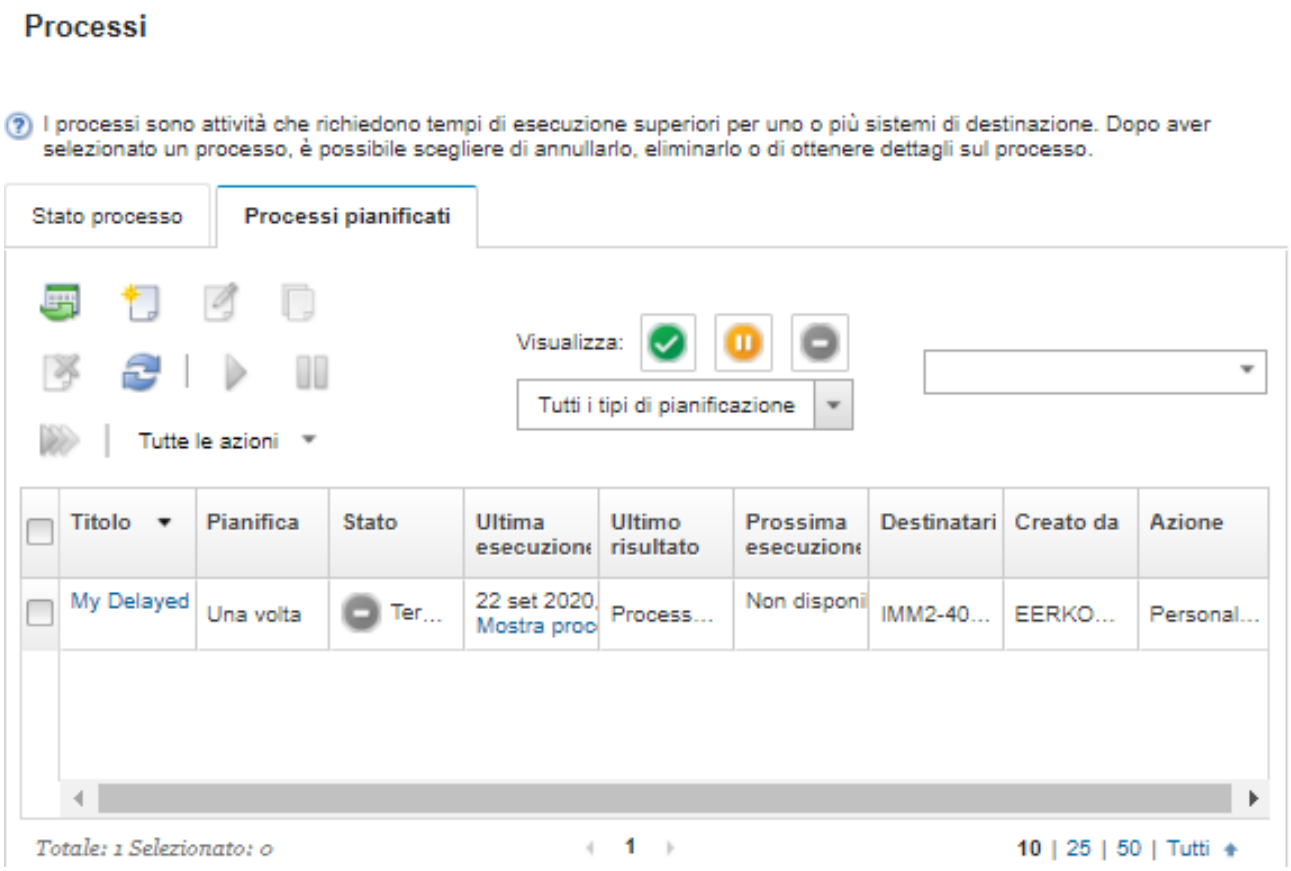
Procedura

Per creare e pianificare un processo, attenersi alla procedura descritta di seguito.

- Per le attività complesse, come l'aggiornamento del firmware e la raccolta dei dati di servizio, creare il processo dalla finestra di dialogo o dalla pagina dell'attività corrente.
  1. Fare clic su **Pianificazione** per creare una pianificazione per l'esecuzione di questa attività. Viene visualizzata la finestra di dialogo Pianifica nuovo processo.
  2. Immettere il nome del processo.
  3. Specificare quando eseguire il processo. Le opzioni disponibili variano a seconda del tipo di processo. Alcuni processi non possono essere periodici o attivati da un evento
     - **Una volta**. Questi processi vengono eseguiti solo una volta. Specificare la data e l'ora in cui si desidera eseguire questo processo.
     - **Periodico**. Questi processi vengono eseguiti più di una volta. Specificare quando e con che frequenza si desidera eseguire questo processo.
     - **Attivato da evento**. Questi processi vengono eseguiti quando si verifica un evento specifico.
       a. Specificare la data e l'ora in cui si desidera eseguire questo processo e fare clic su **Avanti**.
       b. Selezionare l'evento che attiva il processo.
  4. Fare clic su **Crea processo**.
- Per attività semplici, come l'accensione e il riavvio del sistema, creare la pianificazione del processo dalla pagina "Processi".
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Monitor → Processi** e sulla scheda **Processo pianificato** per visualizzare la pagina "Processi pianificati".
  2. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo "Pianifica nuovi processi".
  3. Immettere il nome del processo.
  4. Specificare quando eseguire il processo.
     - **Una volta**. Questi processi vengono eseguiti solo una volta.
       a. Specificare la data e l'ora in cui si desidera eseguire questo processo e fare clic su **Avanti**.
       b. Selezionare i dispositivi gestiti di cui eseguire il processo.
     - **Periodico**. Questi processi vengono eseguiti più di una volta.
       a. Specificare quando e con che frequenza si desidera eseguire questo processo.
       b. Selezionare i dispositivi gestiti di cui eseguire il processo**.**
     - **Attivato da evento**. Questi processi vengono eseguiti quando si verifica un evento specifico.
       a. Specificare la data e l'ora in cui si desidera eseguire questo processo e fare clic su **Avanti**.
       b. Selezionare i dispositivi gestiti di cui eseguire il processo e fare clic su **Avanti**.
       c. Selezionare l'evento che attiva il processo.
  5. Fare clic su **Crea**.

Al termine

Viene visualizzata la scheda Processi pianificati con un elenco di tutte le pianificazioni dei processi in XClarity Administrator.



Da questa pagina, è possibile eseguire le seguenti azioni:

- Per visualizzare le informazioni su tutti i processi attivi e completati per una specifica pianificazione di un processo, fare clic sul collegamento nella colonna **Processo**.
  - Per restringere l'elenco di pianificazioni dei processi visualizzati per un tipo specifico di pianificazione, fare clic su **Tipi di pianificazione** e scegliere tra le seguenti opzioni:
    - **Tutti i tipi di pianificazione**
    - **Una volta**
    - **Periodico**
    - **Attivato**
  - Per nascondere o mostrare solo le pianificazioni dei processi che si trovano in uno stato specifico, fare clic su una delle seguenti icone:
    - Per visualizzare tutti i processi pianificati attivi, fare clic sull'icona **Attivo** icona ( ).
    - Per visualizzare tutti i processi pianificati non attivi, fare clic sull'icona **In pausa** icona ( ).
    - Per visualizzare tutti i processi pianificati già eseguiti, di cui non è stata pianificata una nuova esecuzione, fare clic sull'icona **Terminato** ( ).
  - Elencare solo i processi pianificati che contengono testo specifico immettendo il testo nel campo **Filtro**.
  - Ordinare i processi pianificati per colonna facendo clic su un'intestazione di colonna.

- Per visualizzare l'ultima esecuzione del processo, controllare la colonna **Ultima esecuzione**. Per visualizzare lo stato dell'ultima esecuzione del processo, fare clic sul collegamento "Stato del processo" in questa colonna.
- Per visualizzare quando è pianificata la prossima esecuzione del processo, controllare la colonna **Prossima esecuzione**. Per visualizzare un elenco di tutte le date e gli orari futuri, fare clic sul collegamento "Altro" in questa colonna.
- Per eseguire immediatamente il processo associato alla pianificazione, fare clic sull'icona **Esegui** ().
- Per disabilitare o abilitare la pianificazione di un processo, fare clic rispettivamente sull'icona **Pausa** () o sull'icona **Attiva** ().
- Per copiare e modificare la pianificazione di un processo, fare clic sull'icona **Copia** ().
- Per modificare la pianificazione di un processo, fare clic sull'icona **Modifica** ().
- Per eliminare uno o più pianificazioni del processo selezionato, fare clic sull'icona **Elimina** ().
- Esportare le informazioni sulle pianificazioni di processi specifici selezionando le pianificazioni e facendo clic sull'icona **Esporta come CSV** ().
- Per aggiornare l'elenco delle pianificazione dei processi, fare clic su **Tutte le azioni → Aggiorna**.

Aggiunta di una risoluzione e di commenti a un processo

È possibile aggiungere una risoluzione e i commenti a un processo completato, indipendentemente dallo stato di errore o di riuscita. È possibile eseguire questa operazione per un processo principale e per le attività secondarie del processo.

Procedura

Effettuare una delle seguenti operazioni per aggiungere una risoluzione e i commenti a un processo.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Monitor → Processi** e sulla scheda **Stato dei processi** per visualizzare la pagina Stato dei processi.

Passo 2. Fare clic sul collegamento per il processo nella colonna **Processo** per visualizzare i dettagli del processo.

Passo 3. Fare clic sull'icona **Note** () per visualizzare la finestra di dialogo Note.

Da questa finestra di dialogo, è possibile visualizzare una cronologia di tutte le note e le risoluzioni aggiunte al processo. È possibile cancellare la cronologia facendo clic su **Cancella tutti i record**.

Passo 4. Scegliere una delle seguenti risoluzioni.
- **Nessuna modifica**
- **Analisi in corso**
- **Risolto**
- **Interrotto**

Passo 5. Aggiungere una nota nel campo **Nota**.

Passo 6. Fare clic su **Applica**.

Nella pagina Stato dei processi, La risoluzione viene visualizzata nella colonna **Stato** di questo processo.

Visualizzazione delle relazioni tra processi ed eventi

Un *diagramma di flusso* è una vista grafica che mostra le relazioni tra le attività (inclusi processi ed eventi) che sono state avviate manualmente da un utente o automaticamente da Lenovo XClarity Administrator. Il diagramma di flusso consente di identificare i problemi illustrando la sequenza di azioni inizializzate e gli eventi generati (se generati) con le relative cause.

Prima di iniziare

I flussi delle attività sono disabilitati per impostazione predefinita. È necessario abilitare i flussi delle attività prima di poter generare i flussi per un'attività. È possibile visualizzare i flussi solo per le attività che si verificano quando Flusso attività è abilitato.

Attenzione: I flussi delle attività aumentano l'utilizzo della memoria di XClarity Administrator. Si consiglia di non abilitare i flussi delle attività se l'utilizzo della memoria di XClarity Administrator è già elevato.

Informazioni su questa attività

L'esempio seguente mostra un diagramma di flusso. La sequenza del flusso di eventi da sinistra a destra. Ciascun nodo del flusso rappresenta una singolo attività e include la descrizione, la data e lo stato dell'attività. È possibile posizionare il cursore su titolo del nodo per visualizzare informazioni aggiuntive sull'attività.

Lo stile delle linee tra i nodi indica l'attendibilità della relazione tra i nodi.
- Le linee continue rappresentano un'elevata attendibilità.
- Le righe tratteggiate lunghe rappresentano un'attendibilità media.
- Le righe tratteggiate corte rappresentano un'attendibilità bassa.

Procedura

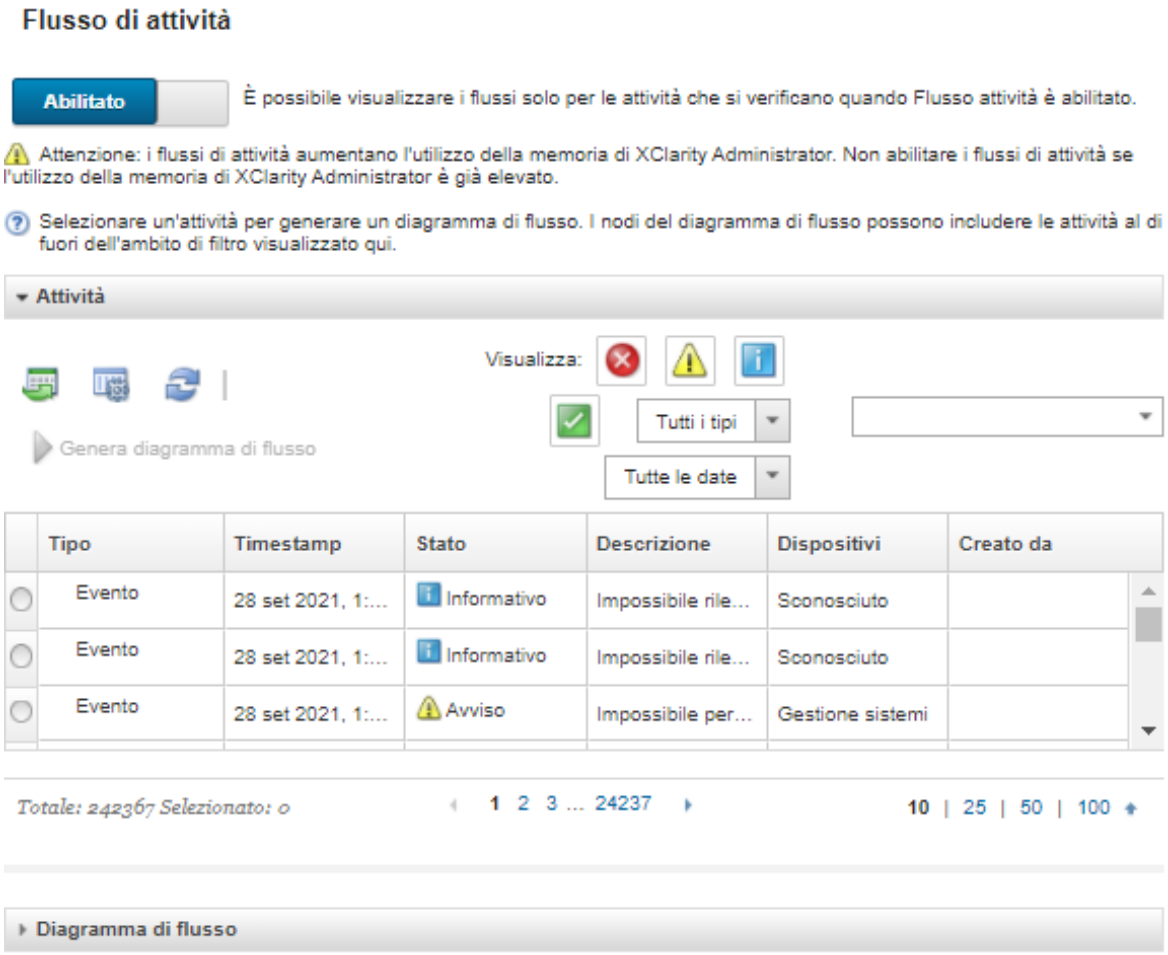
Completare le seguenti operazioni per visualizzare il diagramma di flusso per un'attività specifica.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Monitoraggio → Flusso delle attività** per visualizzare la pagina Flusso delle attività

Passo 2. Abilitare i flussi delle attività selezionando **Abilita flusso delle attività**.

Passo 3. Nella sezione **Attività**, selezionare il processo o l'evento.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di attività specifiche. Inoltre, è possibile selezionare lo stato, il tipo di attività e la data, immettere un filtro personalizzato o del testo (ad esempio, un nome o un indirizzo IP) nel campo **Filtro** ed elencare solo le attività che soddisfano i criteri selezionati.



Passo 4. Fare clic su **Genera diagramma di flusso** per visualizzare il diagramma di flusso nella sezione **Diagramma di flusso**

Al termine

Da questa pagina, è possibile eseguire le seguenti azioni:

- Visualizzare informazioni aggiuntive su ogni attività riportata nel diagramma di flusso posizionando il cursore sull'attività.
- Esportare il flusso relativo alle attività selezionate in un file CSV facendo clic su **Azioni → Esporta in CSV**.

Capitolo 4. Considerazioni sulla gestione

Per la gestione dei dispositivi sono disponibili diverse alternative tra cui scegliere. A seconda dei dispositivi gestiti, potrebbe essere necessario eseguire contemporaneamente diverse soluzioni di gestione.

Un dispositivo può essere gestito da una sola istanza di Lenovo XClarity Administrator. È anche possibile utilizzare un altro software di gestione (come VMware vRealize Operations Manager) con Lenovo XClarity Administrator per *monitorare* i dispositivi gestiti da XClarity Administrator.

Attenzione: Prestare particolare attenzione quando si utilizzano più strumenti di gestione per gestire i dispositivi e prevenire conflitti imprevisti. Ad esempio, l'invio di modifiche dello stato di alimentazione mediante un altro strumento potrebbe determinare un conflitto con i processi di aggiornamento o configurazione in esecuzione su XClarity Administrator.

Dispositivi ThinkSystem, ThinkServer e System x

Se si intende utilizzare un altro software di gestione per monitorare i dispositivi gestiti, creare un nuovo utente locale con le impostazioni SNMP o IPMI corrette dall'interfaccia IMM. Verificare che siano stati concessi i privilegi SNMP o IPMI, a seconda delle specifiche esigenze.

Dispositivi Flex System

Se si intende utilizzare un altro software di gestione per monitorare i dispositivi gestiti e questo software di gestione utilizza la comunicazione SNMPv3 o IPMI, è necessario preparare l'ambiente eseguendo le seguenti operazioni per ciascun modulo CMM gestito:

1. Accedere all'interfaccia Web del controller di gestione dello chassis utilizzando nome utente e password di `RECOVERY_ID`.
2. Se i criteri di sicurezza sono impostati su **Protetto**, modificare il metodo di autenticazione utente.
   a. Fare clic su **Gestione del modulo di gestione → Account utente**.
   b. Fare clic sulla scheda **Account**.
   c. Fare clic su **Impostazioni di login globali**.
   d. Fare clic sulla scheda **Generale**.
   e. Selezionare **Prima autenticazione esterna, poi locale** per il metodo di autenticazione utente.
   f. Fare clic su **OK**.
3. Creare un nuovo utente locale con le impostazioni SNMP o IPMI corrette dall'interfaccia Web del controller di gestione.
4. Se i criteri di sicurezza sono impostati su **Protetto**, scollegarsi e accedere all'interfaccia Web del controller di gestione utilizzando il nuovo nome utente e la password. Quando richiesto, modificare la password per il nuovo utente.

È ora possibile utilizzare il nuovo utente come utente SNMP o IPMI attivo.

Nota: Se si annulla la gestione e quindi si gestisce nuovamente lo chassis, questo nuovo account utente viene bloccato e disabilitato. In questo caso, ripetere queste operazioni per creare un nuovo account utente.

Capitolo 5. Gestione dei gruppi di risorse

È possibile utilizzare il gruppo di risorse in Lenovo XClarity Administrator per creare un insieme logico di dispositivi gestiti, utilizzabile e visualizzabile globalmente.

Ulteriori informazioni: XClarity Administrator: gruppi di risorse

Informazioni su questa attività

Sono disponibili tre tipi di gruppi di risorse:

- **Static**. Gruppo personalizzato di dispositivi specifici.
- **Dinamico**. Gruppo di dispositivi basato su regole (ad esempio, tutti i server di un tipo specifico). Questo gruppo contiene un elenco dinamico di dispositivi basato su una serie di proprietà dell'inventario.

Non è possibile eseguire azioni su un gruppo di risorse. Tuttavia, è possibile selezionare tutti i dispositivi del gruppo ed eseguire le azioni globalmente su tutti i dispositivi selezionati.

Visualizzazione dello stato dei dispositivi in un gruppo di risorse

È possibile visualizzare lo stato di tutti i dispositivi gestiti in un gruppo di risorse.

Informazioni su questa attività

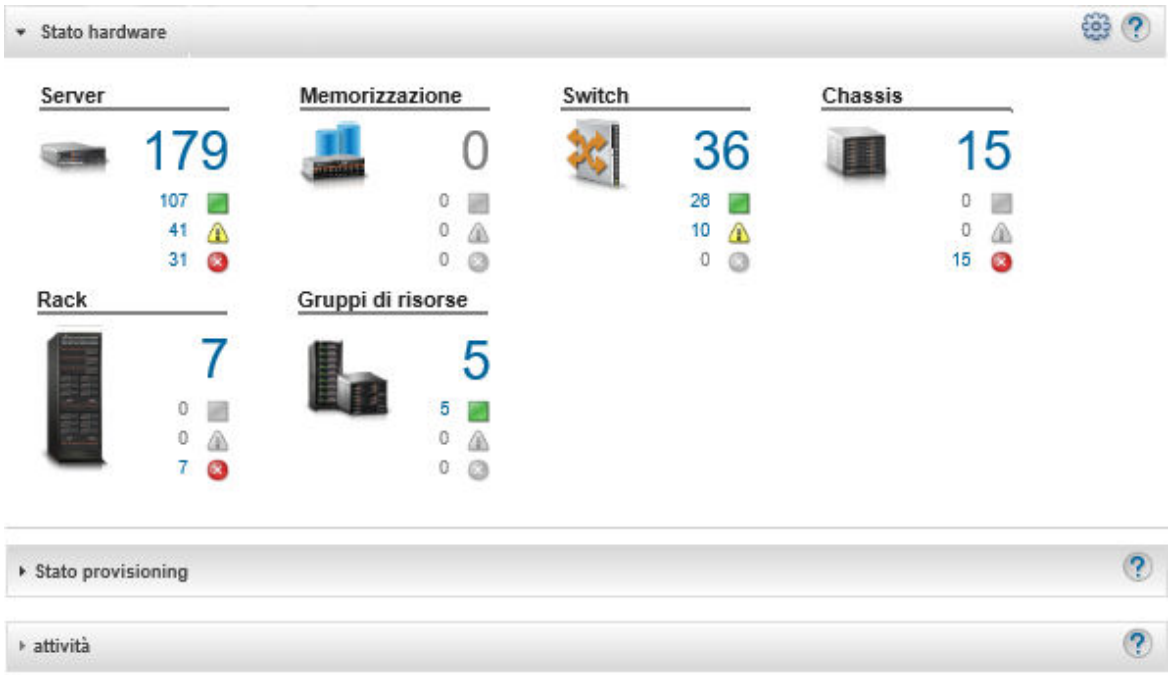
Le seguenti icone di stato vengono utilizzate per indicare l'integrità globale di tutti i dispositivi del gruppo di risorse. L'integrità globale del gruppo indica il dispositivo con gravità più elevata nel gruppo.

- Icona **Critico** ( )
- Icona **Avvertenza** ( )
- Icona **Normale** ( )

Procedura

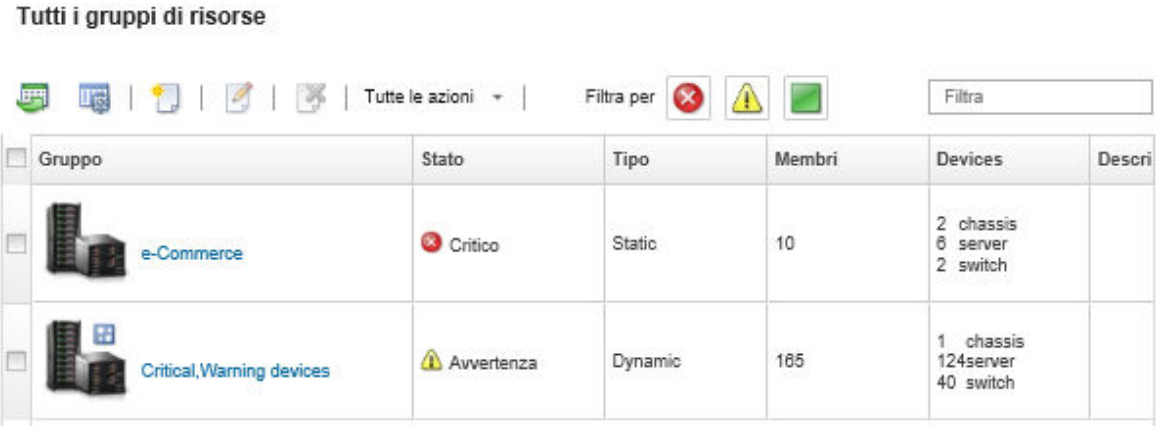
Completare le seguenti operazioni per visualizzare lo stato dei dispositivi di un gruppo di risorse.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Dashboard**. Viene visualizzata la pagina "Dashboard" con una panoramica e lo stato di tutti i dispositivi gestiti e delle altre risorse, inclusi i gruppi di risorse.



Passo 2. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Gruppi di risorse**. Viene visualizzata la pagina Tutti i gruppi di risorse.

Nella pagina "Tutti i gruppi di risorse" viene elencato ogni gruppo di risorse, come nome del gruppo, numero di dispositivi gestiti nel gruppo e stato del dispositivo con gravità più elevata nel gruppo.



Da questa pagina, è possibile eseguire le seguenti azioni:

- Creare un nuovo gruppo di risorse (vedere Creazione di un gruppo di risorse dinamico e Creazione di un gruppo di risorse statico)
- Modificare l'appartenenza del gruppo selezionando un gruppo e facendo clic sull'icona **Modifica** ( ).
- Modificare le proprietà del gruppo selezionando il gruppo e facendo clic su **Tutte le azioni → Modifica proprietà**.
- Rimuovere un gruppo di risorse, selezionando un gruppo e facendo clic sull'icona **Elimina** ( ).

Nota: La rimozione di un gruppo consente di rimuovere solo la definizione del gruppo. Non ha alcun effetto sui dispositivi del gruppo.

- Esportare le informazioni dettagliate su tutti i dispositivi di uno o più gruppi di risorse in un file CSV, facendo clic sull'icona **Esporta** ( ).

Passo 3. Dalla pagina Tutti i gruppi di risorse, fare clic sul nome nella colonna **Gruppi** per visualizzare l'elenco dei dispositivi del gruppo.

Da questa pagina, è possibile eseguire le seguenti azioni:

- Aggiungere o rimuovere i dispositivi in un gruppo di risorse statico facendo clic sull'icona **Modifica** ( ).
- Per visualizzare le informazioni dettagliate su un dispositivo specifico del gruppo di risorse, fare clic sul nome del dispositivo nella colonna **Nome dispositivo**.
- Esportare le informazioni dettagliate su tutti i dispositivi di uno o più gruppi di risorse in un file CSV, facendo clic sull'icona **Esporta** ( ).

Visualizzazione dei membri di un gruppo di risorse

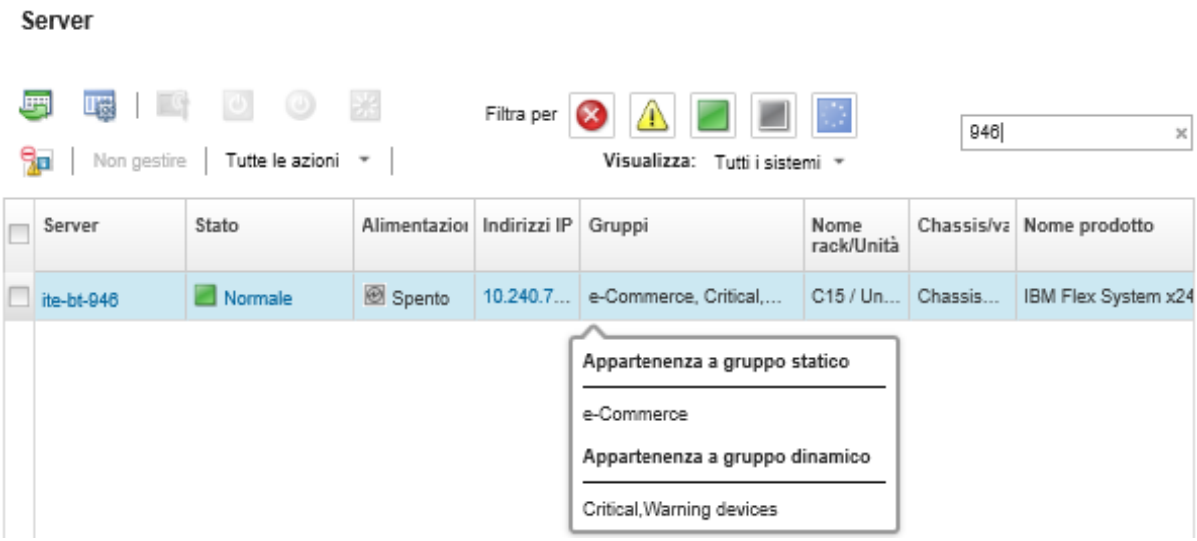
È possibile visualizzare le informazioni dettagliate sui gruppi di risorse, come i membri del gruppo.

Procedura

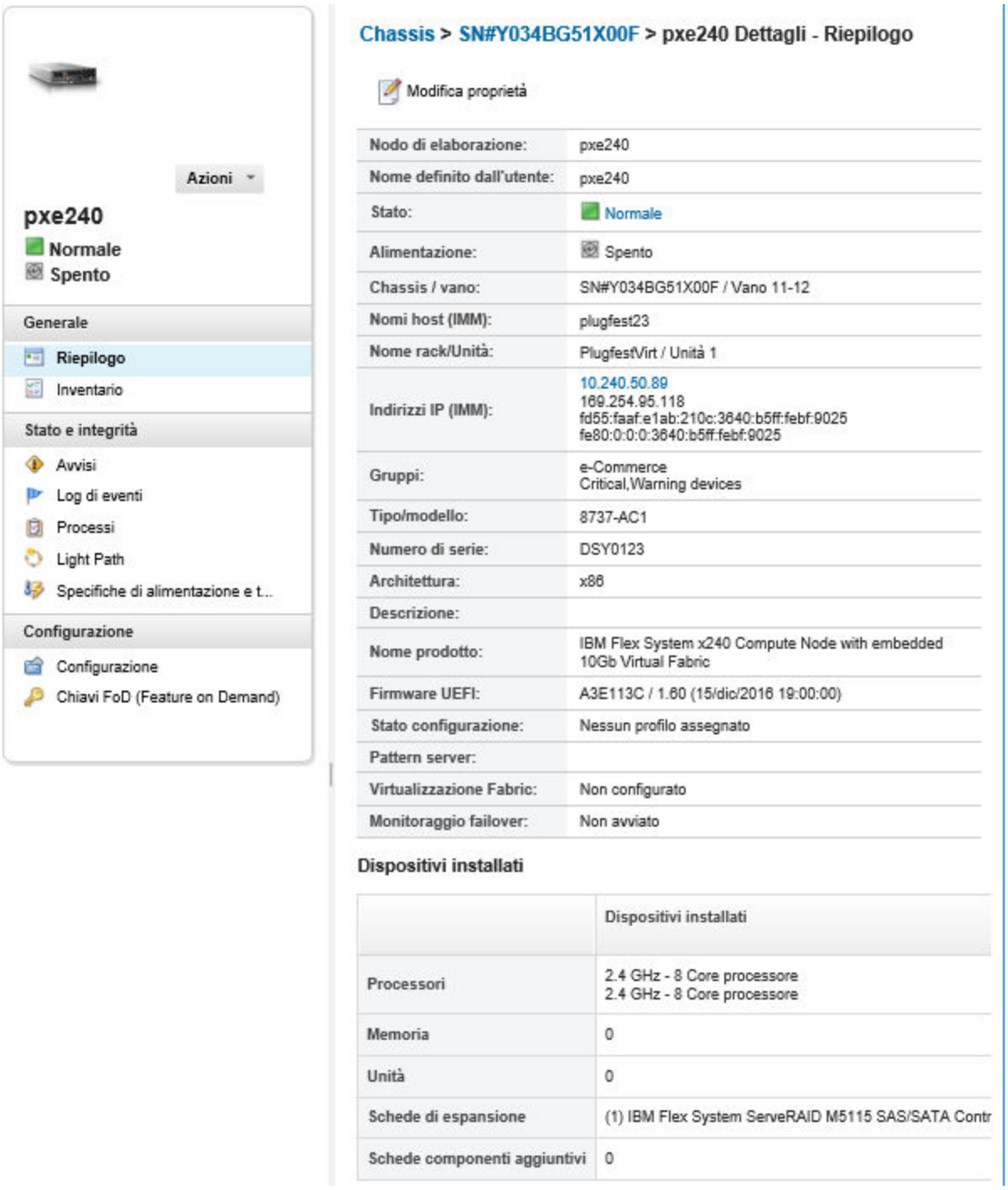
Per visualizzare l'appartenenza di un gruppo, effettuare le seguenti operazioni.

- Per visualizzare tutti i gruppi di cui è membro un dispositivo.
  1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware** e selezionare il tipo di dispositivo per visualizzare la pagina di tutti i dispositivi.

     Passare il mouse sugli elenchi di gruppi nella colonna **Gruppi** per elencare i gruppi di cui è membro il dispositivo.

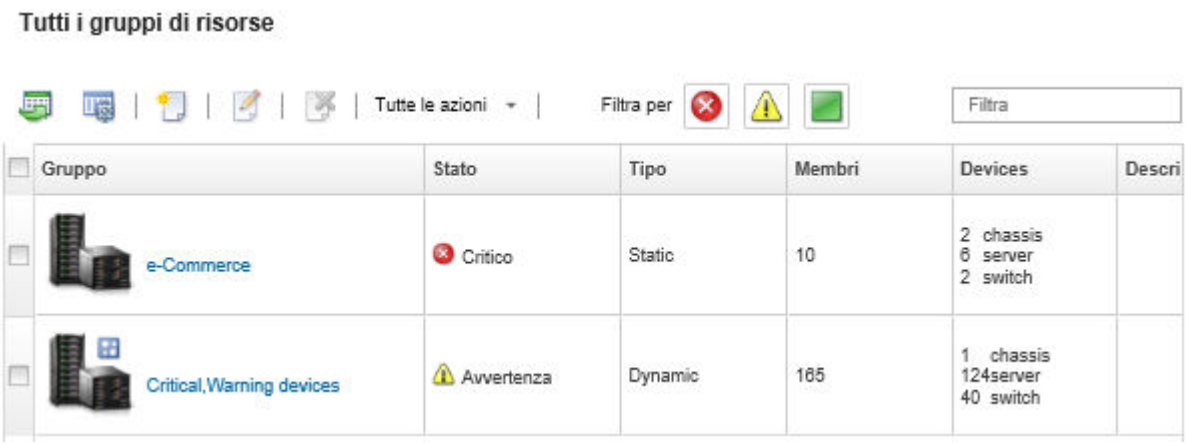


2. Fare clic sul collegamento del nome del dispositivo nella prima colonna. Viene visualizzata la pagina di riepilogo del dispositivo, che include un elenco di gruppi di risorse di cui è membro il dispositivo.



- Per visualizzare i membri di un gruppo.
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Dashboard**. Viene visualizzata la pagina Dashboard con una panoramica e lo stato dei dispositivi gestiti e delle altre risorse, inclusi i rack.
  2. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Gruppi**. Viene visualizzata la pagina "Gruppi di risorse".

     In questa pagina vengono riportati il numero totale di membri e il numero di membro di ciascun tipo di dispositivo del gruppo.



3. Dalla pagina Tutti i gruppi di risorse, fare clic sul nome nella colonna **Gruppi** per visualizzare i dettagli sul gruppo di risorse.

   In questa pagina viene riportato ogni dispositivo membro del gruppo di risorse.

Creazione di un gruppo di risorse dinamico

È possibile creare un gruppo di risorse per una serie dinamica di dispositivi gestiti basato su una serie di criteri.

Informazioni su questa attività

È possibile creare un gruppo di risorse dinamico utilizzando uno o più dei seguenti criteri per ciascun tipo di dispositivo.

Criteri	Chassis	Chassis ad alta densità	Server	Switch Flex System	switch Rack-Switch	Dispositivo di storage
Nome scheda componente aggiuntivo			✓ (tranne ThinkServer)			
Contattare	✓		✓		✓	✓
Descrizione	✓	✓	✓		✓	✓
Nome di dominio completo	✓		✓			

Criteri	Chassis	Chassis ad alta densità	Server	Switch Flex System	switch Rack-Switch	Dispositivo di storage
Nome host	✓		✓	✓	✓	
Indirizzo IPv4*	✓		✓	✓	✓	✓
Indirizzo IPv6	✓		✓	✓	✓	
Posizione	✓	✓	✓		✓	✓
Tipo di macchina	✓		✓	✓	✓	✓
Modello	✓		✓	✓	✓	✓
Stato di integrità globale	✓		✓	✓	✓	✓
Core processore			✓			
Nome prodotto	✓		✓	✓	✓	✓
Rack	✓	✓	✓		✓	✓
Stanza	✓	✓	✓		✓	✓
Nome definito dall'utente	✓	✓	✓	✓	✓	✓

Nota: Per gli indirizzi IPv4, è possibile specificare un singolo indirizzo oppure un intervallo di indirizzi, separati da un trattino oppure utilizzando un asterisco come carattere jolly (ad esempio, `1.1.1.*` o `1.1.1.1-1.1.1.255` senza spazi).

Procedura

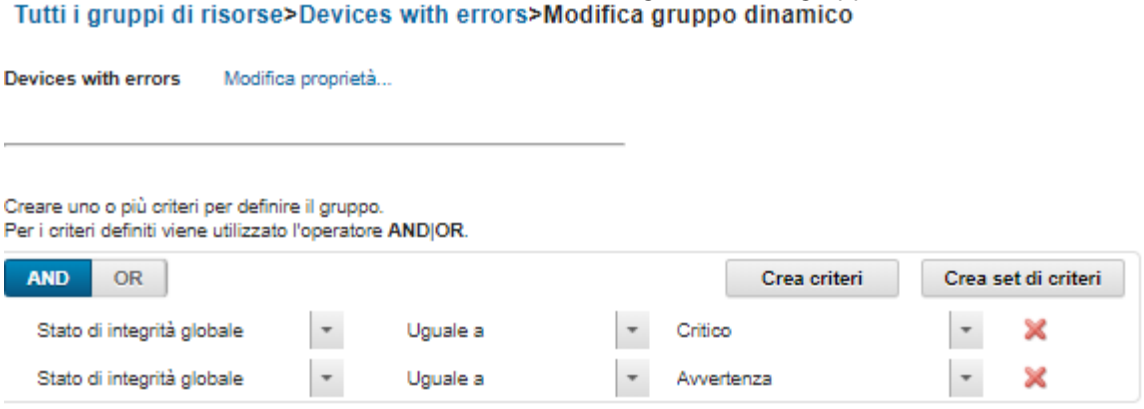
Per creare e popolare un gruppo di risorse dinamico, completare le seguenti operazioni

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware → Gruppi di risorse**. Viene visualizzata la pagina Tutti i gruppi di risorse.

Passo 2. Fare clic sull'icona **Crea** ( ) per creare un gruppo vuoto. Viene visualizzata la finestra di dialogo "Crea gruppo vuoto".

Passo 3. Selezionare **Gruppo dinamico** per raggruppare i dispositivi in base a una serie di criteri.

Passo 4. Fare clic su **Crea**. Viene visualizzata la finestra di dialogo "Modifica gruppo dinamico".



Passo 5. Aggiungere i criteri per questo gruppo dinamico.

- Selezionare l'operatore da utilizzare per la serie di gruppi. É possibile selezionare uno dei seguenti valori:

  - **AND**. I membri devono soddisfare tutti i valori specificati.
  - **OR**. I membri devono soddisfare uno o più dei valori specificati.
- Fare clic su **Crea criteri** per aggiungere una nuova regola di criteri alla serie.
- Fare clic su **Crea serie di criteri** per aggiungere una sottoserie di regole di criteri.

Nota: Nuovi criteri e insieme di criteri vengono sempre aggiunti nella parte inferiore dell'elenco.

Passo 6. Fare clic su **Applica** per salvare i criteri di gruppo e creare il gruppo oppure fare clic su **Anteprima** per visualizzare i dispositivi inclusi nel gruppo, utilizzando i criteri correnti senza creare il gruppo.

Al termine

- È possibile visualizzare quali gruppi di risorse appartengono a un dispositivo dalla colonna **Gruppi** nelle pagine di tutti i dispositivi e di riepilogo dei dispositivi.
- È possibile modificare i criteri del gruppo dinamico selezionando il gruppo di risorse e facendo clic sull'icona **Modifica** ( ).
- È possibile modificare le proprietà del gruppo di risorse facendo clic su **Tutte le azioni → Modifica proprietà**.

Creazione di un gruppo di risorse statico

È possibile creare un gruppo di risorse che contiene una serie personalizzata di dispositivi gestiti.

Procedura

Per creare e popolare un gruppo di risorse statico, completare le seguenti operazioni.

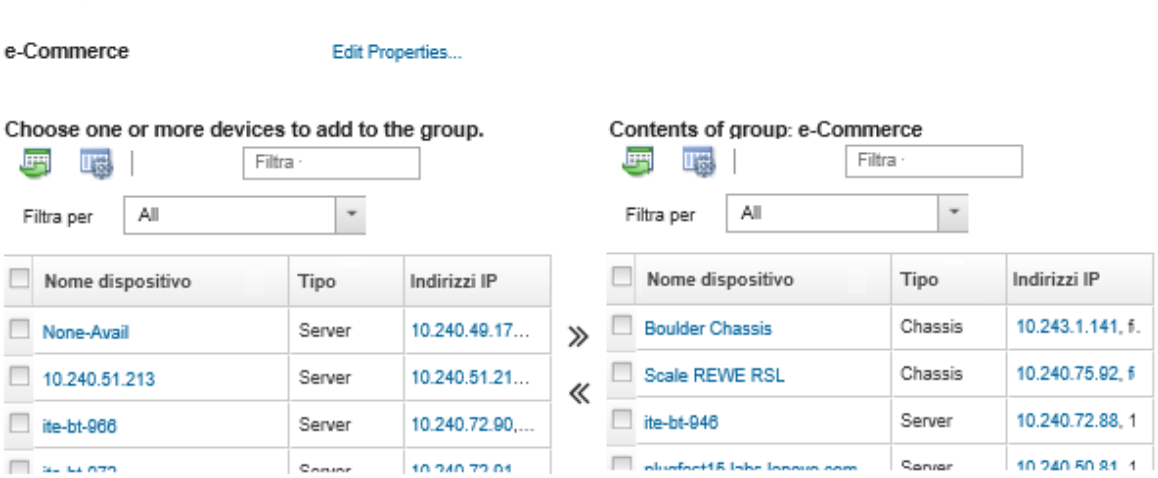
Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware → Gruppi di risorse**. Viene visualizzata la pagina Gruppi di risorse .

Passo 2. Fare clic sull'icona **Crea** ( ) per creare un gruppo vuoto. Viene visualizzata la finestra di dialogo "Crea gruppo vuoto".

Passo 3. Specificare il nome del gruppo e la descrizione facoltativa.

Passo 4. Selezionare **Gruppo statico** per creare un gruppo di dispositivi definiti in modo esplicito.

Passo 5. Fare clic su **Crea**. Viene visualizzata la pagina "Modifica gruppo statico".



Passo 6. Selezionare i dispositivi che si desidera aggiungere al gruppo dall'elenco **Tutti i dispositivi disponibili non presenti nel gruppo** e fare clic sull'icona **Aggiungi** (») per spostare i dispositivi selezionati nell'elenco **Contenuto del gruppo**.

Nota:

- È possibile ordinare gli elenchi per semplificare l'identificazione di specifici dispositivi, facendo clic sulle intestazioni delle colonne. Inoltre, è possibile selezionare un tipo di dispositivo dall'elenco a discesa **Filtra per**, selezionare uno chassis dall'elenco a discesa o immettere il testo (come un nome o un indirizzo IP) nel campo **Filtro** per elencare solo i dispositivi che soddisfano i criteri selezionati
- Se si sceglie di spostare uno chassis nel gruppo, i dispositivi nello chassis non vengono aggiunti automaticamente al gruppo. Per aggiungere tutti i componenti dello chassis al gruppo, selezionare **Chassis → <*chassis_name*>** nel menu a discesa **Mostra** per visualizzare l'elenco di tutti i componenti dello chassis specificato, selezionare la casella di controllo accanto all'intestazione della colonna Nome dispositivo per selezionare tutti i dispositivi e quindi fare clic sull'icona **Aggiungi** (») per spostare i dispositivi selezionati nell'elenco **Contenuto del gruppo**.

Al termine

- È possibile visualizzare quali gruppi di risorse appartengono a un dispositivo dalla colonna **Gruppi** nelle pagine di tutti i dispositivi e di riepilogo dei dispositivi.
- È possibile aggiungere o rimuovere un dispositivo da un gruppo di risorse statico dalle pagine di tutti i dispositivi e dei dettagli del dispositivo, facendo clic su **Tutte le azioni → Gruppi → Aggiungi a gruppo** o **Tutte le azioni → Gruppi → Rimuovi da gruppo**.

  Nota: È possibile aggiungere e rimuovere i dispositivi solo dai gruppi di risorse statici. Non è possibile rimuoverli dai gruppi dinamici.
- È possibile modificare le proprietà del gruppo di risorse facendo clic su **Tutte le azioni → Modifica proprietà**.

Rimozione di un gruppo di risorse

È possibile rimuovere un gruppo di risorse da Lenovo XClarity Administrator.

Informazioni su questa attività

L'eliminazione di un gruppo consente di eliminare solo la definizione del gruppo. Non ha alcun effetto sui dispositivi del gruppo.

Procedura

Completare le seguenti operazioni per rimuovere un gruppo di risorse.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Gruppi di risorse**. Viene visualizzata la pagina Tutti i gruppi di risorse.

Nella pagina "Tutti i gruppi di risorse" viene elencato ogni gruppo di risorse, come nome del gruppo, numero di dispositivi gestiti nel gruppo e stato del dispositivo con gravità più elevata nel gruppo.

Passo 2. Selezionare il gruppo di risorse da rimuovere.

Passo 3. Fare clic sull'icona **Elimina** ( ).

Passo 4. Fare clic su **Elimina**.

Modifica delle proprietà del gruppo di risorse

È possibile modificare le proprietà di un gruppo di risorse specifico.

Procedura

Per modificare le proprietà del gruppo di risorse, procedere come segue

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Gruppi di risorse** per visualizzare la pagina "Tutti i gruppi di risorse"

Passo 2. Selezionare il gruppo di risorse da aggiornare.

Passo 3. Fare clic su **Tutte le azioni → Modifica proprietà** per visualizzare la finestra di dialogo Modifica proprietà del gruppo.

Passo 4. Modificare le seguenti informazioni, in base alle esigenze.
- Nome del gruppo
- Descrizione

Passo 5. Fare clic su **Salva**.

Nota: Quando vengono modificate queste proprietà, è possibile che si verifichi un breve ritardo nella visualizzazione delle modifiche nell'interfaccia Web di XClarity Administrator

Capitolo 6. Gestione dei rack

È possibile utilizzare i rack in Lenovo XClarity Administrator per raggruppare i dispositivi gestiti in modo da riprodurre la configurazione del rack fisico nel data center.

Prima di iniziare

Dopo avere spostato un nodo in un altro chassis, attendere da 5 a 10 minuti prima di tentare di modificare il rack in XClarity Administrator che contiene lo chassis.

Quando si estrae un dispositivo da un rack, il nome del rack e i valori delle unità inferiori del rack vengono cancellati nell'inventario dei dispositivi. I valori di ambiente e posizione non vengono cancellati.

Informazioni su questa attività

In questa procedura viene descritto come creare e popolare in modo interattivo un singolo rack con dispositivi gestiti ed elementi di riempimento.

Se è necessario aggiungere più dispositivi ai rack o modificare numerosi rack, considerare la possibilità di utilizzare un foglio di calcolo per eseguire un'importazione di massa o di implementare uno script PowerShell per automatizzare l'attività. Per ulteriori informazioni sull'utilizzo dell'importazione di massa, vedere Gestione dello chassis e Gestione dei server. Per informazioni sugli script PowerShell, vedere Toolkit PowerShell (LXCAPSTool) nella documentazione online di XClarity Administrator.

XClarity Administrator riconosce le proprietà dei rack definite in un dispositivo gestibile. Quando si gestisce un dispositivo, XClarity Administrator configura le proprietà di sistema del dispositivo e aggiorna la vista rack. Se il rack non esiste in XClarity Administrator, viene creato un nuovo rack e il dispositivo viene aggiunto al nuovo rack.

Nota:

- I serverSystem x3500 M5, NeXtScale nx360 M5, ThinkServer SD350 e tower non sono supportati nella vista rack.
- Per i sistemi complessi scalabili System x3850 X5, è necessario aggiungere singolarmente ciascun nodo (server) al rack.
- Quando XClarity Administrator viene riavviato, l'hardware dimostrativo non è persistente nella vista rack.

Procedura

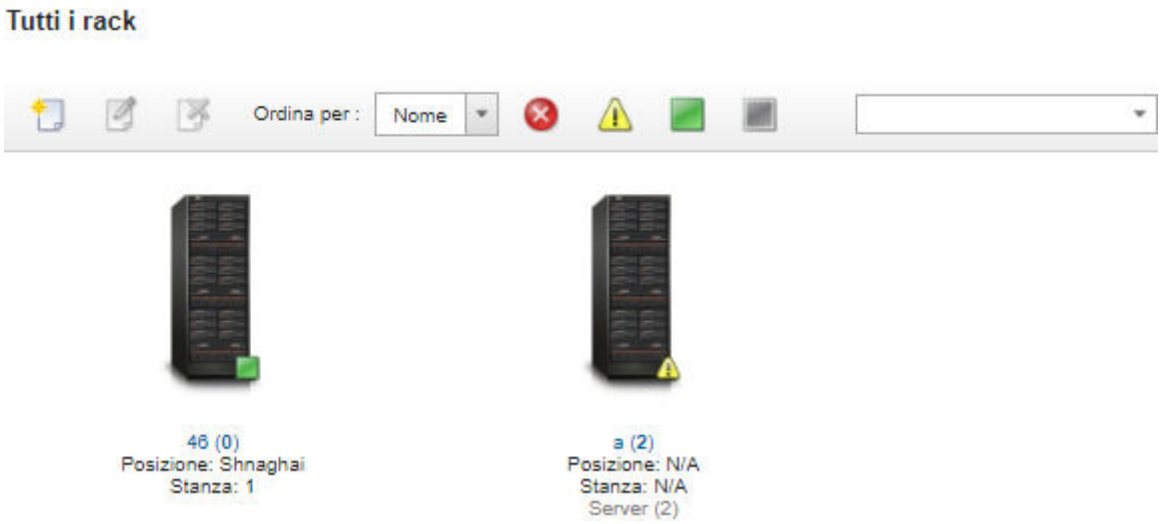
Per creare e popolare i rack, attenersi alla procedura descritta di seguito.

- Creazione e popolazione di un singolo rack con dispositivi gestiti.
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Rack**. Viene visualizzata la pagina Tutti i rack.

     Nella pagina Tutti i rack sono visualizzati i singoli rack come immagine di anteprima con nome del rack, numero di dispositivi gestiti nel rack e stato del dispositivo con gravità più elevata.

     Nota: È possibile filtrare i rack per gravità facendo clic sulle seguenti icone nella barra degli strumenti. È inoltre possibile immettere il nome del rack nel campo **Filtro** per filtrare ulteriormente i rack visualizzati.
     - Icona **Avvisi critici** ()

- Icona **Avvisi di avvertenza** ( )
- Icona **Avvisi normali** ( )

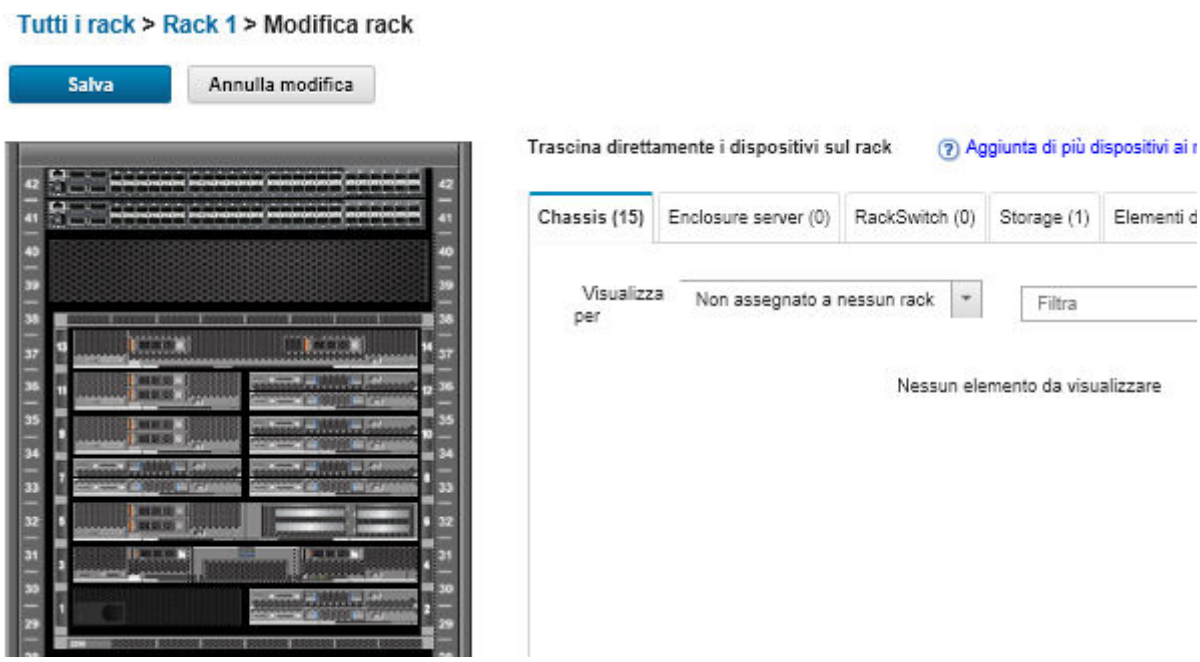


2. Fare clic sull'icona **Crea** ( ) per creare un rack vuoto. Viene visualizzata la finestra di dialogo "Crea rack vuoto".
3. Compilare la finestra di dialogo con nome del rack, altezza, posizione e ambiente.

   Nota:

   - I nomi dei rack non devono essere univoci. È possibile creare rack con lo stesso nome purché la posizione o la sala o entrambe siano differenti.
   - Il nome del rack può includere solo le lettere maiuscole e minuscole, i numeri e i seguenti caratteri speciali: punto (.), trattino (-) e carattere di sottolineatura (_).
   - La posizione può essere costituita da massimo 23 caratteri.
4. Fare clic su **Crea**. Un'immagine di anteprima del nuovo rack viene aggiunta alla pagina Tutti i rack.
5. Fare doppio clic sull'immagine di anteprima del rack. Nella pagina della vista rack vengono visualizzate l'immagine del rack vuoto e le proprietà del rack.

6. Fare clic su **Modifica rack** per visualizzare la pagina Modifica rack.



7. Aggiungere tutti i dispositivi e gli elementi di riempimento appropriati alla vista grafica:

   Nota: Solo i dispositivi gestiti che sono in uno stato "Online" possono essere aggiunti al rack.

   - Fare clic sulla scheda **Chassis** per visualizzare un elenco degli chassis gestiti che non sono stati aggiunti a un rack. Trascinare e rilasciare uno chassis gestito nella posizione desiderata del rack per aggiungere lo chassis al rack.
   - Fare clic sulla scheda **Enclosure server** per visualizzare un elenco di server rack gestiti e di enclosure server a più nodi che non sono stati aggiunti a un rack. Trascinare e rilasciare un server rack o gli enclosure server nella posizione desiderata del rack per aggiungere il server rack al rack.
   - Fare clic sulla scheda **RackSwitch** per visualizzare un elenco di switch RackSwitch gestiti che non sono stati aggiunti a un rack. Trascinare e rilasciare uno switch RackSwitch nella posizione desiderata del rack per aggiungere lo switch al rack.
   - Fare clic sulla scheda **Storage** per visualizzare un elenco di vari dispositivi di storage. Trascinare e rilasciare il dispositivo di storage appropriato nella posizione desiderata del rack per aggiungere il dispositivo di storage al rack.
   - Fare clic sulla scheda **Elementi di riempimento** per visualizzare un elenco di vari elementi di riempimento. Trascinare e rilasciare l'elemento di riempimento appropriato nella posizione desiderata del rack per aggiungere l'elemento di riempimento al rack.

     Un *elemento di riempimento* è qualsiasi dispositivo nel rack che non è gestito da XClarity Administrator. Sono disponibili i seguenti elementi di riempimento:
     - Elementi di riempimento generici
     - Switch rack generici
     - Controller di storage ed enclosure
     - Controller di storage ed enclosure dei partner (come IBM, NetApp ed EMC)

     - Posizione, ambiente, rack e proprietà dell'unità inferiore del rack vengono aggiornati per il dispositivo, quando si aggiungono o rimuovono i dispositivi da un rack.
     - È possibile ordinare l'elenco di dispositivi in ogni scheda utilizzando l'elenco a discesa **Visualizza per**. È inoltre possibile immettere del testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i dispositivi visualizzati.

- È possibile rimuovere i dispositivi gestiti e gli elementi di riempimento dal rack, trascinando e rilasciando gli oggetti fuori dal rack.

8. Fare clic su **Salva** per salvare la configurazione del rack.

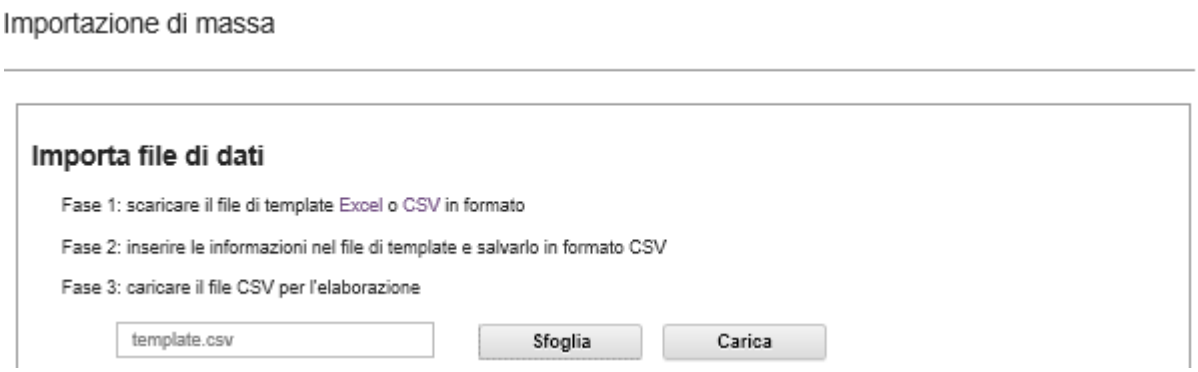
   Il completamento del processo di configurazione potrebbe richiedere diversi minuti. Durante la configurazione, le informazioni su rack e posizione vengono inviate al modulo CMM o al controller di gestione della scheda di base dei dispositivi gestiti.

9. Personalizzare gli elementi di riempimento aggiunti al rack facendo clic sull'elemento di riempimento e quindi su **Modifica proprietà**. Nella finestra di dialogo "Modifica proprietà" è possibile specificare nome, LRU (Lowest Rack Unit) e URL da utilizzare per avviare l'interfaccia utente di gestione del dispositivo.

   Suggerimento: una volta salvata la configurazione del rack, è possibile avviare l'interfaccia utente di gestione di un elemento di riempimento facendo clic sull'elemento di riempimento del rack e quindi sul collegamento **URL di avvio**.

- Creazione e popolazione dei rack mediante un file di importazione di massa.

1. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci.
2. Fare clic su **Importazione di massa**. Viene visualizzata la procedura guidata "Importazione di massa".

3. Fare clic sul collegamento **in Excel** o **in CSV** nella pagina Importa file di dati per scaricare il file di importazione di massa modello in formato Excel o CSV.

   Importante: Il file modello potrebbe cambiare a seconda della versione. Assicurarsi di utilizzare sempre il modello più recente.

4. Compilare il foglio di lavoro dati nel file modello e salvare il file in formato CSV.

   Suggerimento: il modello di Excel include un foglio di lavoro **Dati** e un foglio di lavoro **Leggimi**. Utilizzare il foglio di lavoro **Dati** per immettere i dati del dispositivo. Il foglio di lavoro **Leggimi** fornisce informazioni su come compilare ogni campo del foglio di lavoro **Dati** (inclusi i campi obbligatori) e diversi dati di esempio.

   Importante:

   - I dispositivi sono gestiti nell'ordine indicato nel file di importazione di massa.
   - XClarity Administrator utilizza le informazioni sull'assegnazione del rack definite nella configurazione del dispositivo, quando il dispositivo è gestito. Se si modifica l'assegnazione del rack in XClarity Administrator, XClarity Administrator aggiorna la configurazione del dispositivo. Se si aggiorna la configurazione del dispositivo dopo che il dispositivo è stato gestito, tali modifiche vengono riportate in XClarity Administrator.

– È consigliato ma non richiesto di creare in modo esplicito un rack del foglio di calcolo, prima di assegnare il rack a un dispositivo. Se un rack non viene definito in modo esplicito e il rack non esiste già in XClarity Administrator, le informazioni sull'assegnazione del rack specificate per un dispositivo vengono utilizzate per creare il rack con un'altezza predefinita di 52U.

  Se si desidera utilizzare un'altra altezza per il rack, è necessario definire il rack in modo esplicito nel foglio di calcolo, prima di assegnarlo a un dispositivo.

Per definire i rack nel file di importazione di massa, completare le seguenti colonne richieste.
– (Colonne A) Specificare "rack" per il tipo di dispositivo.
– (Colonne V) Specificare il nome del rack.
– (Colonne X) Specificare l'altezza del rack. Sono supportate le seguenti altezze di rack: 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U e 52U.

La figura seguente mostra un file di importazione di massa di esempio con rack definiti.

A	V	W	X
Type	Rack name	Lowest rack unit	Height
rack	Rack_01		37
rack	Rack_02		52

Nota: È possibile utilizzare lo stesso file di importazione di massa per gestire e aggiungere i dispositivi a un rack (vedere Gestione dei sistemi nella documentazione online di Lenovo XClarity Administrator).

5. Dalla procedura guidata Importazione di massa immettere il nome del file CSV da caricare per l'elaborazione. È possibile fare clic su **Sfoglia** per trovare il file.
6. Fare clic su **Carica** per caricare e convalidare il file.
7. Fare clic su **Avanti** per visualizzare la pagina "Riepilogo immissioni" con un elenco di rack e altri dispositivi da gestire e verificare il riepilogo dei rack e gli altri dispositivi che si desidera gestire.
8. Fare clic su **Avanti** per visualizzare la pagina "Credenziali dispositivi". Fare clic su ciascuna scheda e, facoltativamente, specificare le impostazioni globali e le credenziali da utilizzare per tutti i dispositivi di un tipo specifico. I dispositivi che utilizzeranno le impostazioni globali e le credenziali sono elencati sul lato destro di ciascuna scheda.
9. Fare clic su **Gestisci**. Viene visualizzata la pagina "Risultati monitoraggio" con informazioni sullo stato della gestione di ciascun dispositivo nel file di importazione di massa.

   Viene creato un processo per il processo di gestione. Se si chiude la procedura guidata di importazione di massa, il processo di gestione continua in background. È possibile monitorare lo stato del processo di gestione dal log dei processi. Per ulteriori informazioni sul log processi, vedere "Monitoraggio dei processi" a pagina 172.

Al termine

È possibile modificare la preferenza dell'ordine di numerazione dei rack (vedere Impostazioni preferenze inventario).

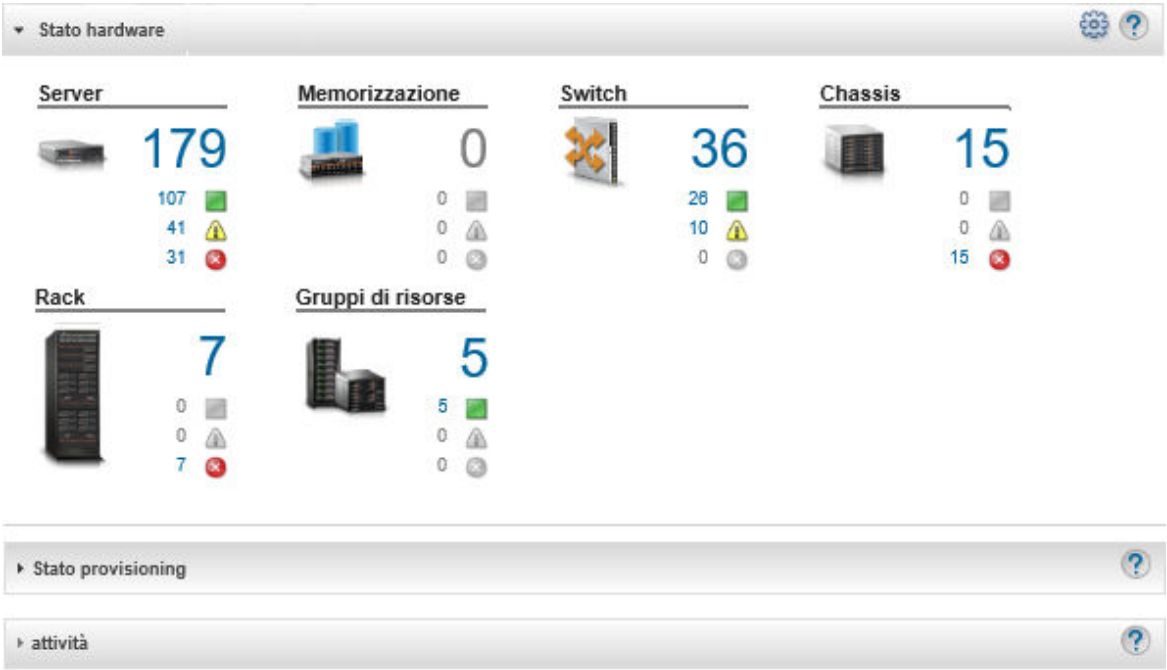
Visualizzazione dello stato dei dispositivi di un rack

Per ogni rack, è possibile visualizzare lo stato di tutti i dispositivi gestiti nel rack.

Procedura

Completare una o più delle seguenti azioni per visualizzare lo stato di tutti i dispositivi di un rack.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Dashboard**. Viene visualizzata la pagina Dashboard con una panoramica e lo stato dei dispositivi gestiti e delle altre risorse, inclusi i rack.

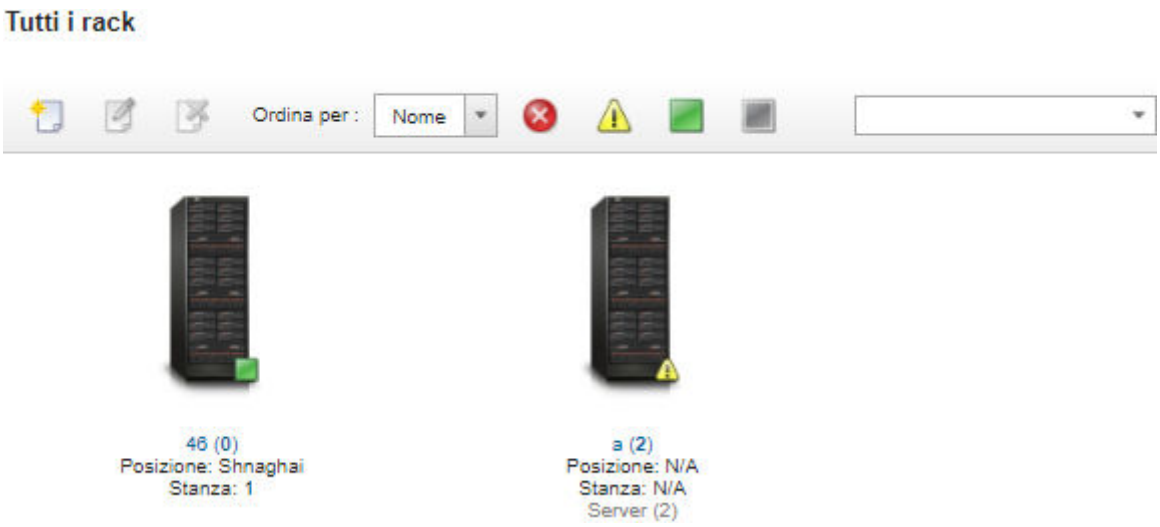


Passo 2. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Rack**. Viene visualizzata la pagina Rack.

Nella pagina Rack sono visualizzati i singoli rack come immagine di anteprima con nome del rack, numero di dispositivi gestiti nel rack e stato del dispositivo con gravità più elevata.

Nota: È possibile ordinare l'elenco per nome del rack, numero di dispositivi nel rack o per gravità per semplificare l'identificazione di rack specifici. L'elenco viene ordinato da sinistra a destra, dall'alto verso il basso. Inoltre, è possibile filtrare i rack per gravità facendo clic sulle seguenti icone nella barra degli strumenti oppure immettere un nome del rack nel campo **Filtro** per filtrare ulteriormente i rack visualizzati.

- Icona **Avvisi critici** ( )
- Icona **Avvisi di avvertenza** ( )
- Icona **Avvisi normali** ( )



Passo 3. Dalla pagina Tutti i rack, fare clic sul nome del rack o doppio clic su un'anteprima del rack per visualizzare la vista grafica e le proprietà del rack.

La *vista rack* è una vista grafica della parte anteriore del rack che mostra i dispositivi nel rack, come chassis, server rack, switch TOC (Top-Of-Rack) ed elementi di riempimento. Un'icona di stato su ogni dispositivo indica lo stato corrente del dispositivo.

Da questa pagina, è possibile eseguire le seguenti azioni:

- Aggiungere o rimuovere i dispositivi al rack facendo clic su **Modifica rack**.

  Nota: Quando vengono cambiati i componenti del rack, potrebbe verificarsi un breve ritardo nella visualizzazione delle informazioni nell'interfaccia XClarity Administrator.
- Modificare le proprietà di dispositivo e filtro (come nome, posizione e URL per avviare l'interfaccia Web di gestione) facendo clic sul dispositivo o sull'elemento di riempimento e quindi su **Modifica proprietà** nel riquadro di riepilogo del dispositivo.
- Visualizzare l'interfaccia Web del controller di gestione per un dispositivo o un elemento di riempimento facendo clic sul dispositivo o sull'elemento di riempimento e quindi sul collegamento **URL di avvio** nel riquadro di riepilogo del dispositivo.

Passo 4. Visualizzare il riepilogo o lo stato dettagliato di un dispositivo o di un componente:

a. Fare clic sul dispositivo o sul componente del rack per visualizzare il riepilogo dello stato, le proprietà e lo stato del dispositivo o del componente.

b. Fare doppio clic su un dispositivo per visualizzare la pagina dei dettagli del dispositivo.

Procedura

È possibile modificare la preferenza dell'ordine di numerazione dei rack (vedere Impostazioni preferenze inventario).

Rimozione di un rack

È possibile rimuovere un rack da Lenovo XClarity Administrator.

Procedura

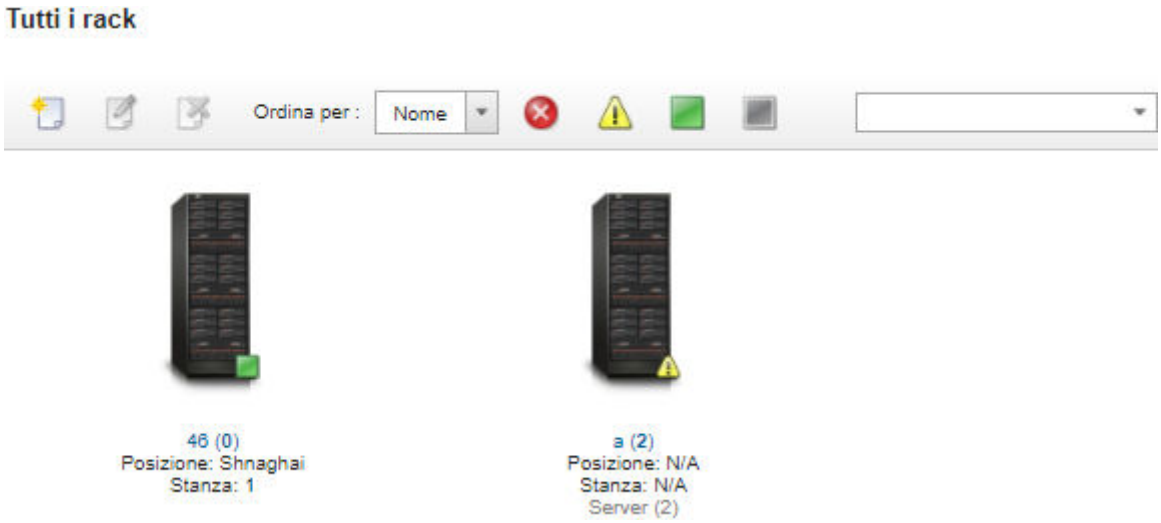
Completare le seguenti operazioni per rimuovere un rack.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Rack**. Viene visualizzata la pagina Tutti i rack.

Nella pagina Tutti i rack sono visualizzati i singoli rack come immagine di anteprima con nome del rack, numero di dispositivi gestiti nel rack e stato del dispositivo con gravità più elevata.

Nota: È possibile ordinare l'elenco per nome del rack, numero di dispositivi nel rack o per gravità per semplificare l'identificazione di rack specifici. L'elenco viene ordinato da sinistra a destra, dall'alto verso il basso. Inoltre, è possibile filtrare i rack per gravità facendo clic sulle seguenti icone nella barra degli strumenti oppure immettere un nome del rack nel campo **Filtro** per filtrare ulteriormente i rack visualizzati.

- Icona **Avvisi critici** ( )
- Icona **Avvisi di avvertenza** ( )
- Icona **Avvisi normali** ( )



Passo 2. Selezionare l'anteprima del rack da rimuovere.

Passo 3. Fare clic sull'icona **Rimuovi** ( ).

Passo 4. Fare clic su **Rimuovi**.

Risultati

L'anteprima del rack viene rimossa dalla pagina Tutti i rack e tutti i dispositivi presenti nel rack possono ora essere inclusi in un altro rack dalla pagina Modifica rack.

Capitolo 7. Gestione dello chassis

Lenovo XClarity Administrator è in grado di gestire diversi tipi di sistemi, incluso lo chassis di Flex System.

Ulteriori informazioni:  XClarity Administrator: rilevamento

Prima di iniziare

Nota: I componenti dello chassis (come CMM, nodi di elaborazione Flex e switch Flex) vengono rilevati e gestiti automaticamente quando si gestisce lo chassis che li contiene. Non è possibile rilevare e gestire componenti dello chassis separati.

Prima di gestire lo chassis, accertarsi di aver soddisfatto le seguenti condizioni:

- Prima di gestire un dispositivo, osservare le relative considerazioni di gestione. Per informazioni, vedere Considerazioni sulla gestione nella documentazione online di XClarity Administrator.
- Affinché lo chassis possa essere gestito, alcune porte devono essere disponibili per la comunicazione con il modulo CMM. Accertarsi che queste porte siano disponibili prima di gestire uno chassis. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.
- Accertarsi che il firmware minimo richiesto sia installato in ciascuno chassis che si desidera gestire mediante XClarity Administrator. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.
- Verificare che l'impostazione **Numero di sessioni attive simultanee per utenti LDAP** in CMM sia impostata su 0 (zero) per lo chassis. È possibile verificare questa impostazione dall'interfaccia Web CMM facendo clic su **Gestione del modulo di gestione → Account utente**, **Impostazioni di login globali**, quindi sulla scheda **Generale**.
- Verificare che vi siano almeno tre sessioni della modalità comando TCP impostate per la comunicazione fuori banda con CMM. Per informazioni sull'impostazione del numero di sessioni, vedere Comando tcpcmdmode nella documentazione online del modulo CMM.
- Per individuare uno chassis situato in una sottorete *differente da* XClarity Administrator, assicurarsi che una delle seguenti condizioni venga soddisfatta:
  - Verificare che sia abilitato l'inoltro SLP multicast sugli switch TOR (Top-of-Rack) e sui router del proprio ambiente. Consultare la documentazione fornita con lo switch o il router specifico per determinare se l'inoltro SLP multicast è abilitato e per reperire le procedure necessarie per abilitarlo qualora sia disabilitato.
  - Se SLP è disabilitato sull'endpoint o nella rete, in alternativa è possibile utilizzare il metodo di rilevamento DNS, aggiungendo manualmente un record di servizio (record SRV) al server DNS (Domain Name Server), ad esempio per XClarity Administrator.
    ```
    _lxca._tcp.labs.lenovo.com      service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```
    Quindi, abilitare il rilevamento DNS sul modulo CMM dall'interfaccia Web di gestione, facendo clic su **Gestione del modulo di gestione → Protocollo di rete** e sulla scheda **DNS**, selezionando **Utilizza DNS per rilevare Lenovo XClarity Administrator**.

    Nota:

    - Il livello di firmware del modulo CMM deve essere aggiornato a maggio 2017 per supportare il rilevamento automatico mediante DNS.

– Se nell'ambiente sono presenti più istanze di XClarity Administrator, lo chassis viene rilevato solo dalla prima istanza che risponde alla richiesta di rilevamento. Lo chassis non viene rilevato da tutte le istanze.

Implementare indirizzi IPv4 *o* IPv6 per tutti i moduli CMM e gli switch Flex gestiti da XClarity Administrator. Se si implementa IPv4 per alcuni CMM e switch Flex e IPv6 per altri, alcuni eventi potrebbero non essere ricevuti nel log di controllo (o come trap di controllo).

Attenzione: Se si intende aggiornare i moduli CMM che eseguono una release di stack Flex con livello firmware compreso tra 1.3.2.1 2PET12K e 2PET12Q, in esecuzione da oltre tre settimane e con una configurazione a doppio CMM, è necessario riposizionare virtualmente entrambi i moduli CMM prima di aggiornare il firmware con XClarity Administrator.

Importante: Se oltre a Lenovo XClarity Administrator si intende utilizzare un altro software di gestione per monitorare lo chassis, e tale software di gestione utilizza la comunicazione SNMPv3, è necessario prima creare un ID utente CMM locale configurato con le informazioni SNMPv3 appropriate, poi eseguire il login al CMM utilizzando tale ID utente, quindi modificare la password. Per ulteriori informazioni, vedere Considerazioni sulla gestione nella documentazione online di XClarity Administrator.

Informazioni su questa attività

XClarity Administrator è in grado di rilevare automaticamente gli chassis nell'ambiente dell'utente individuando i sistemi gestibili che si trovano nella stessa sottorete IP di XClarity Administrator. Per rilevare gli chassis presenti in altre sottoreti, specificare un indirizzo IP o un intervallo di indirizzi IP oppure importare le informazioni da un foglio di calcolo.

Una volta che gli chassis sono stati gestiti da XClarity Administrator, XClarity Administrator esegue periodicamente il polling di ciascuno chassis gestito per raccogliere informazioni, quali inventario, VPD (Vital Product Data) e stato. È possibile visualizzare e monitorare ogni chassis gestito ed eseguire azioni di gestione (come la configurazione delle informazioni di sistema, dell'impostazione di rete e del failover). Per gli chassis in modalità protetta le azioni di gestione sono disabilitate.

Gli chassis sono gestiti mediante l'autenticazione gestita di *XClarity Administrator*.

Per impostazione predefinita, i dispositivi vengono gestiti utilizzando l'autenticazione gestita di XClarity Administrator per eseguire il login ai dispositivi. Quando si gestiscono i server rack e lo chassis Lenovo, è possibile scegliere di utilizzare l'autenticazione locale o gestita per eseguire il login ai dispositivi.

- Quando l'*autenticazione locale* viene utilizzata per i server rack, lo chassis Lenovo e gli switch rack Lenovo, XClarity Administrator utilizza una credenziale memorizzata per eseguire l'autenticazione al dispositivo. La *credenziale memorizzata* può essere un account utente attivo sul dispositivo o un account utente in un server Active Directory.

  Prima di gestire il dispositivo utilizzando l'autenticazione locale è necessario creare le credenziali memorizzate in XClarity Administrator che corrispondono a un account utente attivo sul dispositivo o un account utente in un server Active Directory (vedere Gestione delle credenziali memorizzate nella documentazione online di XClarity Administrator).

  Nota:

  – I dispositivi RackSwitch supportano solo le credenziali memorizzate per l'autenticazione. Le credenziali utente di XClarity Administrator non sono supportate.
- L'*autenticazione gestita* consente di gestire e monitorare più dispositivi utilizzando le credenziali del server di autenticazione XClarity Administrator invece delle credenziali locali. Quando l'autenticazione gestita viene utilizzata per un dispositivo (diverso dai server ThinkServer e System x M4 o dagli switch), XClarity

Administrator configura il dispositivo gestito e i relativi componenti installati per utilizzare il server di autenticazione XClarity Administrator per la gestione centralizzata.

- Quando è abilitata l'autenticazione gestita, è possibile gestire i dispositivi utilizzando le credenziali memorizzate o inserite manualmente (vedere Gestione degli account utente e nella documentazione online di XClarity Administrator).

  La credenziale memorizzata viene utilizzata solo finché XClarity Administrator non configura le impostazioni LDAP sul dispositivo. Successivamente, eventuali modifiche delle credenziali memorizzate non incidono sulla gestione o sul monitoraggio di tale dispositivo.

  Nota: Quando è abilitata l'autenticazione gestita per un dispositivo, non è possibile modificare le credenziali memorizzate per tale dispositivo utilizzando XClarity Administrator.
- Se viene utilizzato un server LDAP esterno o locale come server di autenticazione XClarity Administrator, gli account utente definiti nel server di autenticazione vengono utilizzati per eseguire il login a XClarity Administrator, CMM e controller di gestione della scheda di base nel dominio di XClarity Administrator. Gli account utente del controller di gestione e CMM locali sono disabilitati.
- Se viene utilizzato un provider di identità SAML 2.0 come server di autenticazione XClarity Administrator, gli account SAML non saranno accessibili per i dispositivi gestiti. Tuttavia quando si utilizzano un provider di identità SAML e un server LDAP insieme, se il provider di identità utilizza gli account esistenti nel server LDAP, gli account utente LDAP possono essere utilizzati per eseguire il login ai dispositivi gestiti mentre i metodi di autenticazione più avanzati forniti da SAML 2.0 (come autenticazione a più fattori e Single Sign-On) possono essere utilizzati per eseguire il login a XClarity Administrator.
- La funzione Single Sign-On consente a un utente già connesso a XClarity Administrator di eseguire automaticamente il login al controllo di gestione della scheda di base. L'opzione Single Sign-On è abilitata per impostazione predefinita quando un server ThinkSystem o ThinkAgile viene inserito nella gestione da XClarity Administrator (a meno che il server non sia gestito con password CyberArk). È possibile configurare l'impostazione globale per abilitare o disabilitare la funzione Single Sign-On per tutti i server ThinkSystem e ThinkAgile gestiti. L'abilitazione dell'opzione Single Sign-On per un server ThinkSystem o ThinkAgile specifico ha la precedenza sull'impostazione globale per tutti i server ThinkSystem e ThinkAgile (vedere).

  Nota: Single Sign-On viene disabilitato automaticamente quando si utilizza il sistema di gestione delle identità CyberArk per l'autenticazione.
- Quando l'autenticazione gestita è abilitata per i server ThinkSystem SR635 e SR655:
  - Il firmware del controller di gestione della scheda di base supporta fino a cinque ruoli utente LDAP. XClarity Administrator aggiunge questi ruoli utente LDAP ai server durante la gestione: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** e **lxc-os-admin**.

    È necessario assegnare gli utenti ad almeno uno dei ruoli utente LDAP specificati per comunicare con i server ThinkSystem SR635 e SR655.
  - Il firmware del controller di gestione non supporta gli utenti LDAP con lo stesso nome utente locale del server.
- Per i server ThinkServer e System x M4, il server di autenticazione XClarity Administrator non viene utilizzato. Di contro, viene creato un account IPMI sul dispositivo con il prefisso "LXCA_", seguito da una stringa casuale. (Gli account utente IPMI locali esistenti non vengono disabilitati). Quando si annulla la gestione di un server ThinkServer, l'account utente "LXCA_" viene disabilitato e il prefisso "LXCA_" viene sostituito con il prefisso "DISABLED_". Per determinare se un server ThinkServer è gestito da un'altra istanza, XClarity Administrator verifica gli account IPMI con il prefisso "LXCA_". Se si sceglie di forzare la gestione di un server ThinkServer gestito, tutti gli account IPMI del dispositivo con il prefisso "LXCA_" vengono disabilitati e rinominati. Valutare la possibilità di cancellare manualmente gli account IPMI non più in uso.

Se si utilizzano credenziali inserite manualmente, XClarity Administrator crea automaticamente una credenziale memorizzata e la utilizza per gestire il dispositivo.

Nota: Quando è abilitata l'autenticazione gestita per un dispositivo, non è possibile modificare le credenziali memorizzate per tale dispositivo utilizzando XClarity Administrator.

- Ogni volta che si gestisce un dispositivo utilizzando le credenziali inserite manualmente, viene creata una nuova credenziale memorizzata per tale dispositivo, anche se è stata creata un'altra credenziale memorizzata per il dispositivo durante un processo di gestione precedente.
- Quando si annulla la gestione di un dispositivo, XClarity Administrator non elimina le credenziali memorizzate create automaticamente per tale dispositivo durante il processo di gestione.

Un dispositivo può essere gestito da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza iniziale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator. Se si verifica un errore durante il processo di annullamento della gestione, sarà possibile selezionare l'opzione **Forza gestione** durante la gestione nella nuova istanza di XClarity Administrator.

Nota: Quando si analizza la rete alla ricerca di dispositivi gestibili, XClarity Administrator non è in grado di sapere se un dispositivo è già gestito da un altro gestore fino a quando non avrà tentato di gestirlo.

Durante il processo di gestione, XClarity Administrator effettua le azioni seguenti:

- Esegue il login allo chassis utilizzando le credenziali fornite.
- Raccoglie l'inventario per tutti i componenti in ogni chassis, come CMM, nodi di elaborazione, dispositivi di storage e Switch Flex.

  Nota: Alcuni dati di inventario vengono raccolti dopo il completamento del processo di gestione. Lo chassis rimarrà nello stato In sospeso finché non verranno raccolti tutti i dati di inventario. Non sarà possibile eseguire determinate attività su un dispositivo gestito (ad esempio la distribuzione di un pattern server) finché non verranno raccolti tutti i dati di inventario del dispositivo e lo chassis non sarà più nello stato In sospeso.
- Configura le impostazioni per il server NTP in modo che tutti i dispositivi gestiti utilizzino il server NTP da XClarity Administrator.
- Assegna gli ultimi criteri di conformità del firmware modificati allo chassis.
- Per i dispositivi Lenovo Flex configura facoltativamente le regole del firewall dei dispositivi per far sì che le richieste in entrata vengano accettate solo da XClarity Administrator.
- Scambia i certificati di sicurezza con CMM, copiando il certificato di sicurezza CMM nell'archivio attendibile di XClarity Administrator e inviando il certificato di sicurezza CA di XClarity Administrator a CMM. CMM carica il certificato nell'archivio attendibile CMM e lo distribuisce ai processori di servizio dei nodi di elaborazione per l'aggiunta nei rispettivi archivi attendibili.
- Configura autenticazione gestita. Le impostazioni per il client LDAP CMM vengono modificate per poter utilizzare XClarity Administrator come server di autenticazione e le impostazioni di login globali nel modulo CMM vengono modificate in **Impostazioni solo per il server di autenticazione esterna**. Per ulteriori informazioni sull'autenticazione gestita, vedere Gestione del server di autenticazione.
- Crea l'account utente di ripristino (`RECOVERY_ID`). Per ulteriori informazioni sull'account `RECOVERY_ID`, vedere Gestione del server di autenticazione.

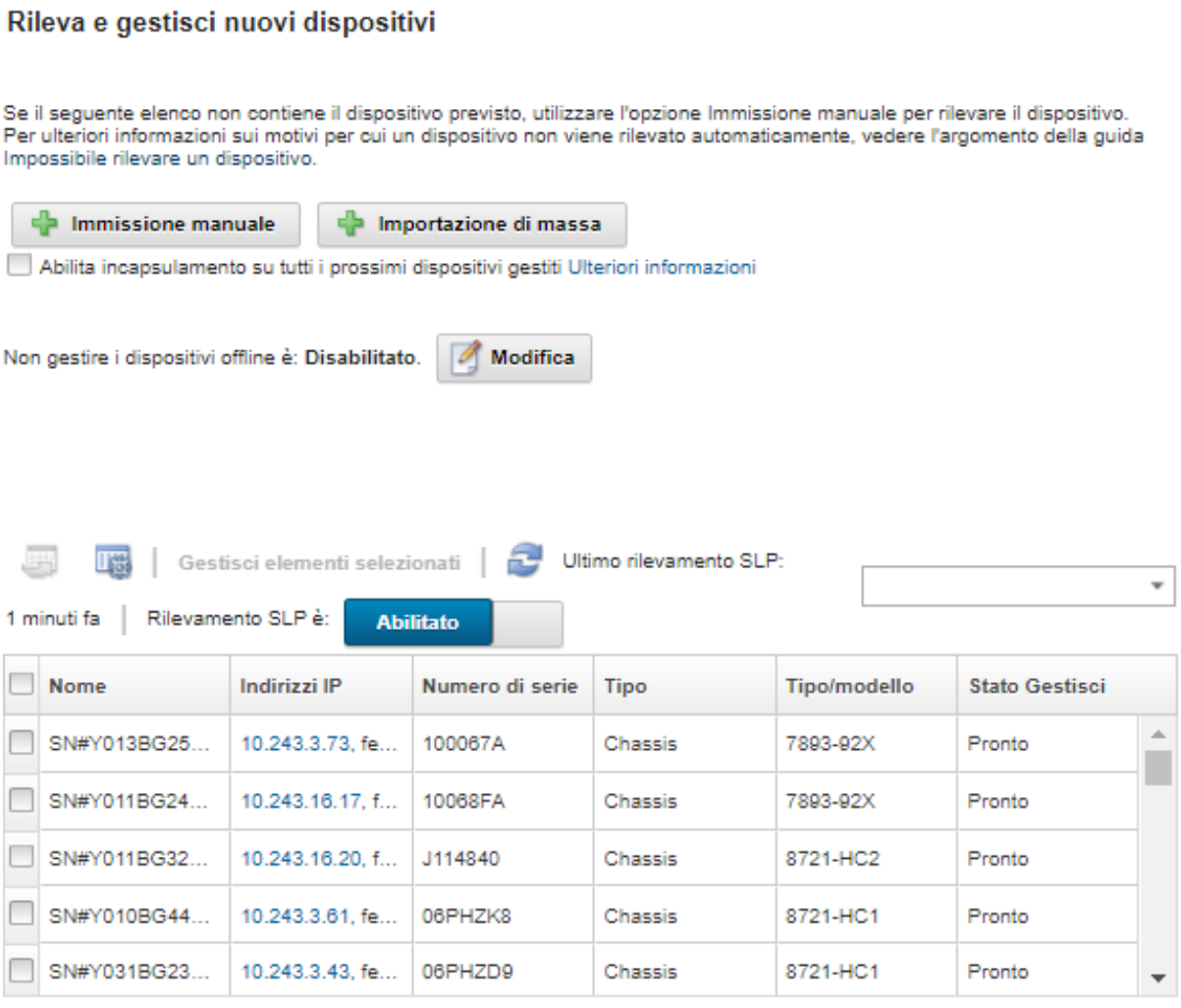
Attenzione: Quando si gestisce uno chassis, XClarity Administrator modifica il numero massimo di connessioni simultanee della modalità comando TCP sicuro portandolo a 15 e imposta il numero massimo di connessioni simultanee della modalità comando TCP legacy su 0. Questo consente di sovrascrivere le impostazioni che potrebbero essere già state impostate su CMM.

Nota: XClarity Administrator non modifica le impostazioni di sicurezza o crittografiche (la modalità crittografica e la modalità utilizzata per le comunicazioni sicure) durante il processo di gestione. Una volta gestito lo chassis, sarà possibile modificare le impostazioni crittografiche (vedere Configurazione delle impostazioni di crittografia sul server di gestione).

Procedura

Per rilevare e gestire lo chassis mediante XClarity Administrator, attenersi a una delle procedure descritte di seguito.

- Rilevare e gestire un numero elevato di chassis e altri dispositivi tramite un file di importazione di massa (vedere Gestione dei sistemi nella documentazione online di Lenovo XClarity Administrator).
- Rilevare e gestire gli chassis che si trovano nella stessa sottorete IP di XClarity Administrator.
  1. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci nuovi dispositivi.



È possibile ordinare le colonne della tabella per individuare più facilmente gli chassis che si desidera gestire. Inoltre, è possibile immettere testo (ad esempio, un nome di sistema o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli chassis visualizzati. È possibile modificare le colonne visualizzate e l'ordinamento predefinito facendo clic sull'icona **Personalizza colonne** ( ).

2. Fare clic sull'icona **Aggiorna** () per rilevare tutti i dispositivi gestibili nel dominio di XClarity Administrator. Il rilevamento potrebbe richiedere diversi minuti.
3. Fare clic sulla casella di controllo **Abilita incapsulamento su tutti i prossimi dispositivi gestiti** per modificare le regole del firewall su tutti i dispositivi durante il processo di gestione affinché le richieste in entrata vengano accettate solo da XClarity Administrator.

   L'incapsulamento può essere abilitato o disabilitato su dispositivi specifici dopo che sono stati gestiti.

   Attenzione: Se l'incapsulamento è abilitato e XClarity Administrator non è più disponibile prima che la gestione di un dispositivo venga annullata, è necessario eseguire la procedura per disabilitare l'incapsulamento al fine di stabilire la comunicazione con il dispositivo. Per le procedure di ripristino, vedere lenovoMgrAlert.mib file e Ripristino della gestione con un modulo CMM dopo un errore del server di gestione.
4. Selezionare uno o più chassis che si desidera gestire.
5. Fare clic su **Gestisci elementi selezionati**.
6. Scegliere di utilizzare l'autenticazione gestita o locale di XClarity Administrator per questo dispositivo. L'autenticazione gestita viene selezionata per impostazione predefinita. Per utilizzare l'autenticazione locale, deselezionare **Autenticazione gestita**.

   Nota: Le autenticazioni locale e gestita non sono supportate per i server ThinkServer e System x M4.
7. Scegliere il tipo di credenziali da utilizzare per il dispositivo e specificare le credenziali appropriate:
   - **Utilizza credenziali immesse manualmente**
     - Specificare l'ID utente locale e la password con autorità **lxc-supervisor** per l'autenticazione al modulo CMM.
     - (Facoltativo) Specificare una nuova password per l'account utente CMM, se la password del dispositivo è scaduta.
   - **Utilizza credenziali memorizzate**

     Selezionare la credenziale memorizzata con autorità **lxc-supervisor** da utilizzare per il dispositivo gestito. È possibile aggiungere le credenziali memorizzate facendo clic su **Gestisci credenziali memorizzate**.

     Nota: Se si sceglie di utilizzare l'autenticazione locale, è necessario selezionare una credenziale memorizzata per gestire il dispositivo.

   Suggerimento: per gestire il dispositivo si consiglia di utilizzare un account di supervisore o amministratore. Se viene utilizzato un account con autorità di livello inferiore, la gestione potrebbe avere esito negativo oppure potrebbe riuscire ma le altre operazioni XClarity Administrator future potrebbero non riuscire sul dispositivo (in particolar modo se il dispositivo viene gestito senza l'autenticazione gestita).

   Per ulteriori informazioni sulle credenziali normali e memorizzate, vedere Gestione degli account utente e Gestione delle credenziali memorizzate.
8. Specificare la password di ripristino, se è selezionata l'autenticazione gestita.

   Un account di ripristino (`RECOVERY_ID`) viene creato sul modulo CMM e tutti gli utenti locali vengono disabilitati. Se si verifica un problema e XClarity Administrator smette di funzionare, *non* sarà possibile eseguire il login al modulo CMM utilizzando i normali account utente. Tuttavia, è possibile eseguire il login utilizzando l'account `RECOVERY_ID`.

   Nota:

   - La password di ripristino è obbligatoria se si sceglie di utilizzare l'autenticazione gestita e non è consentita se si sceglie di utilizzare l'autenticazione locale.

- È possibile scegliere di utilizzare un account di ripristino locale o le credenziali di ripristino memorizzate. In entrambi i casi, il nome utente è sempre `RECOVERY_ID`.
- Verificare che la password rispetti i criteri di sicurezza e delle password per il dispositivo. I criteri di sicurezza e delle password possono variare.
- Assicurarsi di registrare la password di ripristino per gli usi futuri.

Per ulteriori informazioni sull'ID di ripristino, vedere Gestione del server di autenticazione.

9. Fare clic su **Modifica** per modificare i gruppi di ruoli che devono essere assegnati ai dispositivi.

   Nota:

   - È possibile selezionare un elenco dei gruppi di ruoli assegnati all'utente corrente.
   - Se non si modificano i gruppi di ruoli, vengono utilizzati i gruppi di ruoli predefiniti. Per ulteriori informazioni sui gruppi di ruoli predefiniti, vedere Modifica delle autorizzazioni predefinite.

10. Fare clic su **Gestisci**.

    Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Per garantire il completamento del processo, monitorarne l'avanzamento.

    Una volta completato il processo, nella finestra di dialogo verranno visualizzati il numero di dispositivi nello chassis e lo stato dello chassis.

    Nota: Alcuni dati di inventario vengono raccolti dopo il completamento del processo di gestione. Lo chassis rimarrà nello stato In sospeso finché non verranno raccolti tutti i dati di inventario. Non sarà possibile eseguire determinate attività su un dispositivo gestito (ad esempio la distribuzione di un pattern server) finché non verranno raccolti tutti i dati di inventario del dispositivo e lo chassis non sarà più nello stato In sospeso.

11. Al termine del processo, fare clic su **OK**.

    Il dispositivo è ora gestito da XClarity Administrator, che effettua periodicamente il polling automatico del dispositivo gestito per raccogliere informazioni aggiornate, ad esempio l'inventario.

    Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione **Forza gestione**.

    - Se l'istanza XClarity Administrator di gestione è in errore e non è possibile effettuare il ripristino.

      Nota: se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabile) e l'opzione **Forza gestione**.
    - Se l'istanza XClarity Administrator di gestione è stata disattivata prima di avere annullato la gestione dei dispositivi.
    - Se la gestione dei dispositivi non è stata annullata correttamente.

    Attenzione: I dispositivi possono essere gestiti da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza originale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator.

12. Se questo è un nuovo chassis, fare clic su **Continua con la configurazione dello chassis** per convalidare e modificare le impostazioni di rete di gestione per l'intero chassis (inclusi nodi di elaborazione e switch Flex) e per configurare le informazioni del nodo di elaborazione, lo storage locale, gli adattatori I/O, le destinazioni avvio e le impostazioni del firmware creando e distribuendo i pattern server. Per ulteriori informazioni, vedere Modifica delle impostazioni IP di gestione per uno chassis e Configurazione dei server mediante i pattern di configurazione.

- Per rilevare e gestire gli chassis che non si trovano nella stessa sottorete IP di XClarity Administrator, specificare manualmente gli indirizzi IP.
  1. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci.
  2. Fare clic sulla casella di controllo **Abilita incapsulamento su tutti i prossimi dispositivi gestiti** per modificare le regole del firewall su tutti i dispositivi durante il processo di gestione affinché le richieste in entrata vengano accettate solo da XClarity Administrator.

     L'incapsulamento può essere abilitato o disabilitato su dispositivi specifici dopo che sono stati gestiti.

     Attenzione: Se l'incapsulamento è abilitato e XClarity Administrator non è più disponibile prima che la gestione di un dispositivo venga annullata, è necessario eseguire la procedura per disabilitare l'incapsulamento al fine di stabilire la comunicazione con il dispositivo. Per le procedure di ripristino, vedere lenovoMgrAlert.mib file e Ripristino della gestione con un modulo CMM dopo un errore del server di gestione.
  3. Selezionare **Immissione manuale**.
  4. Specificare gli indirizzi di rete degli chassis che si desidera gestire:
     - Fare clic su **Singolo sistema** e immettere un singolo nome di dominio dell'indirizzo IP o il nome di dominio completo (FQDN).

       Nota: Per specificare un FQDN, assicurarsi che nella pagina Accesso alla rete sia specificato un nome di dominio valido (vedere Configurazione dell'accesso alla rete).
     - Fare clic su **Più sistemi** e immettere un intervallo indirizzi IP. Per aggiungere un altro intervallo, fare clic sull'icona **Aggiungi** (). Per rimuovere un intervallo, fare clic sull'icona **Rimuovi** ().
  5. Fare clic su **OK**.
  6. Scegliere di utilizzare l'autenticazione gestita o locale di XClarity Administrator per questo dispositivo. L'autenticazione gestita viene selezionata per impostazione predefinita. Per utilizzare l'autenticazione locale, deselezionare **Autenticazione gestita**.

     Nota: Le autenticazioni locale e gestita non sono supportate per i server ThinkServer e System x M4.
  7. Scegliere il tipo di credenziali da utilizzare per il dispositivo e specificare le credenziali appropriate:
     - **Utilizza credenziali immesse manualmente**
       - Specificare l'ID utente locale e la password con autorità **lxc-supervisor** per l'autenticazione al modulo CMM.
       - (Facoltativo) Specificare una nuova password per l'account utente CMM, se la password del dispositivo è scaduta.
     - **Utilizza credenziali memorizzate**

       Selezionare la credenziale memorizzata con autorità **lxc-supervisor** da utilizzare per il dispositivo gestito. È possibile aggiungere le credenziali memorizzate facendo clic su **Gestisci credenziali memorizzate**.

       Nota: Se si sceglie di utilizzare l'autenticazione locale, è necessario selezionare una credenziale memorizzata per gestire il dispositivo.

     Suggerimento: per gestire il dispositivo si consiglia di utilizzare un account di supervisore o amministratore. Se viene utilizzato un account con autorità di livello inferiore, la gestione potrebbe avere esito negativo oppure potrebbe riuscire ma le altre operazioni XClarity Administrator future potrebbero non riuscire sul dispositivo (in particolar modo se il dispositivo viene gestito senza l'autenticazione gestita).

Per ulteriori informazioni sulle credenziali normali e memorizzate, vedere Gestione degli account utente e Gestione delle credenziali memorizzate.

8. Specificare la password di ripristino, se è selezionata l'autenticazione gestita.

   Un account di ripristino (RECOVERY_ID) viene creato sul modulo CMM e tutti gli utenti locali vengono disabilitati. Se si verifica un problema e XClarity Administrator smette di funzionare, *non* sarà possibile eseguire il login al modulo CMM utilizzando i normali account utente. Tuttavia, è possibile eseguire il login utilizzando l'account RECOVERY_ID.

   Nota:

   – La password di ripristino è obbligatoria se si sceglie di utilizzare l'autenticazione gestita e non è consentita se si sceglie di utilizzare l'autenticazione locale.
   – È possibile scegliere di utilizzare un account di ripristino locale o le credenziali di ripristino memorizzate. In entrambi i casi, il nome utente è sempre RECOVERY_ID.
   – Verificare che la password rispetti i criteri di sicurezza e delle password per il dispositivo. I criteri di sicurezza e delle password possono variare.
   – Assicurarsi di registrare la password di ripristino per gli usi futuri.

   Per ulteriori informazioni sull'ID di ripristino, vedere Gestione del server di autenticazione.

9. Fare clic su **Modifica** per modificare i gruppi di ruoli che devono essere assegnati ai dispositivi.

   Nota:

   – È possibile selezionare un elenco dei gruppi di ruoli assegnati all'utente corrente.
   – Se non si modificano i gruppi di ruoli, vengono utilizzati i gruppi di ruoli predefiniti. Per ulteriori informazioni sui gruppi di ruoli predefiniti, vedere Modifica delle autorizzazioni predefinite.

10. Fare clic su **Gestisci**.

    Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Monitorare l'avanzamento per garantire il completamento del processo.

    Una volta completato il processo, nella finestra di dialogo verrà visualizzato il numero di dispositivi nello chassis e lo stato dello chassis.

    Nota: Alcuni dati di inventario vengono raccolti dopo il completamento del processo di gestione. Lo chassis rimarrà nello stato In sospeso finché non verranno raccolti tutti i dati di inventario. Non sarà possibile eseguire determinate attività su un dispositivo gestito (ad esempio la distribuzione di un pattern server) finché non verranno raccolti tutti i dati di inventario del dispositivo e lo chassis non sarà più nello stato In sospeso.

11. Al termine del processo, fare clic su **OK**.

    Il dispositivo è ora gestito da XClarity Administrator, che effettua periodicamente il polling automatico del dispositivo gestito per raccogliere informazioni aggiornate, ad esempio l'inventario.

    Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione **Forza gestione**.

    – Se l'istanza XClarity Administrator di gestione è in errore e non è possibile effettuare il ripristino.

      Nota: se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabile) e l'opzione **Forza gestione**.
    – Se l'istanza XClarity Administrator di gestione è stata disattivata prima di avere annullato la gestione dei dispositivi.
    – Se la gestione dei dispositivi non è stata annullata correttamente.

Attenzione: I dispositivi possono essere gestiti da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza originale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator.

12. Se questo è un nuovo chassis, fare clic su **Continua con la configurazione dello chassis** per convalidare e modificare le impostazioni di rete di gestione per l'intero chassis (inclusi nodi di elaborazione e switch Flex) e per configurare le informazioni del nodo di elaborazione, lo storage locale, gli adattatori I/O, le destinazioni avvio e le impostazioni del firmware creando e distribuendo i pattern server. Per ulteriori informazioni, vedere Modifica delle impostazioni IP di gestione per uno chassis e Configurazione dei server mediante i pattern di configurazione.

Al termine

- Rilevare e gestire dispositivi aggiuntivi.
- Distribuire le immagini del sistema operativo nei server in cui non è installato alcun sistema operativo. Per ulteriori informazioni, vedere Installazione dei sistemi operativi sui server bare metal.
- Aggiornare il firmware sui dispositivi non conformi ai criteri correnti (vedere Aggiornamento del firmware sui dispositivi gestiti).
- Aggiungere i nuovi dispositivi gestiti al rack appropriato per riflettere l'ambiente fisico (vedere Gestione dei rack).
- Monitorare lo stato dell'hardware e i dettagli (vedere Visualizzazione dello stato di un server gestito).
- Monitorare eventi e avvisi (vedere Utilizzo degli eventi e Gestione degli avvisi).

Visualizzazione dello stato di uno chassis gestito

Da Lenovo XClarity Administrator è possibile visualizzare un riepilogo e lo stato dettagliato degli chassis gestiti e dei relativi componenti installati.

Ulteriori informazioni:

- XClarity Administrator: inventario
- XClarity Administrator: monitoraggio

Informazioni su questa attività

Le seguenti icone di stato vengono utilizzate per indicare l'integrità complessiva del dispositivo. Se i certificati non corrispondono, "(Non attendibile)" viene aggiunto allo stato di ciascun dispositivo applicabile, ad esempio Avvertenza (non attendibile). Se si verifica un problema di connettività o una connessione al dispositivo non è attendibile, "(Connettività)" viene aggiunto allo stato di ciascun dispositivo applicabile, ad esempio Avvertenza (Connettività).

- ( ) Critico
- ( ) Avvertenza
- ( ) In sospeso
- ( ) Informativo
- ( ) Normale
- ( ) Offline
- ( ) Sconosciuto

Procedura

Per visualizzare lo stato di uno chassis gestito, completare le seguenti operazioni.

- Visualizzare le informazioni dettagliate sullo chassis facendo clic sul collegamento **Dettagli** o su **Azioni → Viste → Dettagli**.
- Avviare l'interfaccia Web CMM per lo chassis facendo clic sul collegamento **Indirizzo IP** (vedere Avvio dell'interfaccia Web CMM per uno chassis).
- Modificare le informazioni (ad esempio la descrizione, la posizione e il contatto del supporto) facendo clic su **Azioni → Inventario → Modifica proprietà**.
- Modificare le impostazioni IP di gestione per l'intero chassis, tra cui i nodi di elaborazione e gli switch Flex, facendo clic su **Azioni → Inventario → Modifica indirizzi IP di gestione**.
- Esportare le informazioni dettagliate su uno o più chassis in un unico file CSV selezionando lo chassis e facendo clic su **Azioni → Inventario → Esporta inventario**.

  Nota: è possibile esportare i dati di inventario per un massimo di 60 dispositivi alla volta.

  Suggerimento: Durante l'importazione di un file CSV in Microsoft Excel, i valori di testo contenenti solo numeri vengono trattati come valori numerici (ad esempio nel caso degli UUID). Impostare la formattazione di ogni cella come testo per risolvere il problema.
- Risolvere i problemi che potrebbero verificarsi tra il certificato di sicurezza di Lenovo XClarity Administrator e quello del modulo CMM nello chassis selezionando uno chassis e facendo clic su **Azioni → Sicurezza → Risolvi certificati non attendibili**.

Visualizzazione dei dettagli di uno chassis gestito

È possibile visualizzare le informazioni dettagliate sullo chassis gestito da Lenovo XClarity Administrator, tra cui i livelli di firmware, gli indirizzi IP e l'identificatore univoco universale (UUID, Universally Unique Identifier).

Ulteriori informazioni:

- XClarity Administrator: inventario
- XClarity Administrator: monitoraggio

Informazioni su questa attività

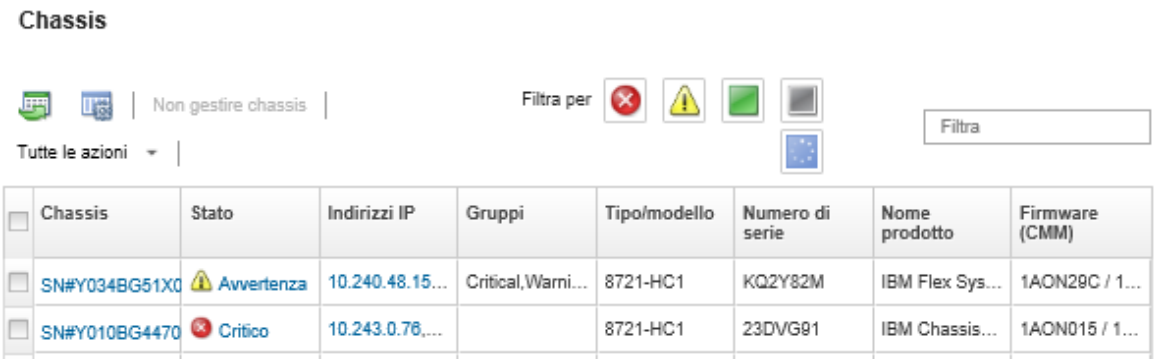
La temperatura dell'aria a livello di sistema viene misurata con un sensore fisico nella parte anteriore del server. Rappresenta la temperatura dell'aria in ingresso del server. La temperatura dell'aria riportata da XClarity Administrator e quella riportata da CMM potrebbero differire se viene acquisita in momenti diversi.

Procedura

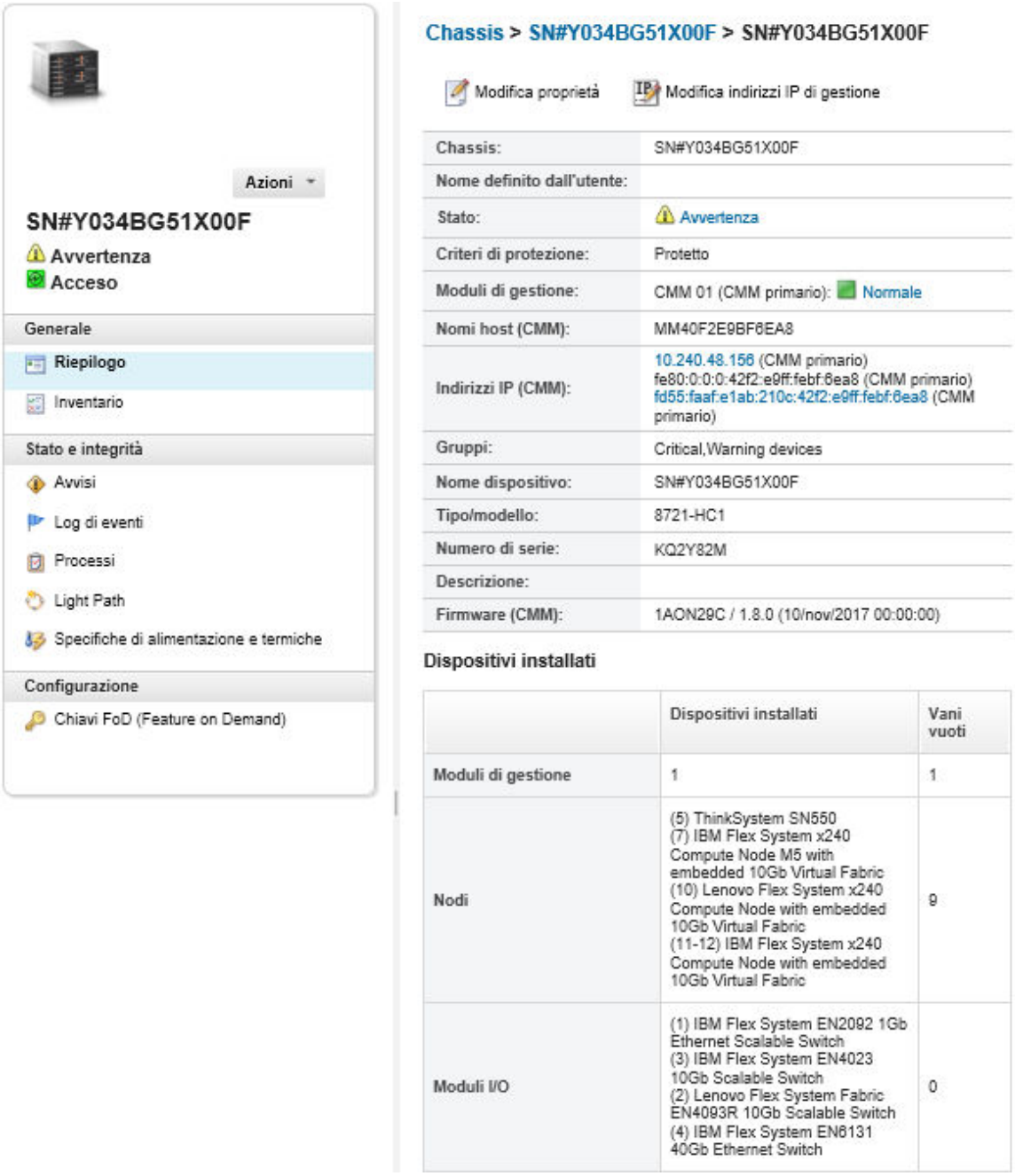
Per visualizzare i dettagli relativi a uno chassis gestito, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Chassis**. Viene visualizzata la pagina Chassis che contiene una vista tabulare di tutti gli chassis gestiti.

È possibile ordinare le colonne della tabella per individuare più facilmente gli chassis che si desidera gestire. Inoltre, è possibile immettere testo (ad esempio, un nome di chassis o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli chassis visualizzati.



Passo 2. Fare clic sul nome dello chassis nella colonna **Chassis**. Viene visualizzata la pagina di riepilogo dello stato relativa allo chassis selezionato, che mostra le proprietà dello chassis e i componenti installati nello chassis.



Passo 3. Completare una o più azioni seguenti:

- Fare clic su **Riepilogo** per visualizzare un riepilogo dello chassis, incluse le informazioni di sistema e i componenti installati (vedere Visualizzazione dello stato di uno chassis gestito).
- Fare clic su **Dettagli inventario** per visualizzare i dettagli sui componenti dello chassis, tra cui:
  - I livelli di firmware per tutti i componenti nello chassis.
  - I dettagli del modulo CMM, ad esempio il nome host, l'indirizzo IPv4, l'indirizzo IPv6 e gli indirizzi MAC.
  - I dettagli relativi alla risorsa dello chassis e del modulo CMM installato nello chassis, tra cui il nome, l'identificatore univoco universale (UUID) e la posizione.
- Fare clic su **Avvisi** per visualizzare l'elenco di avvisi correnti per lo chassis selezionato (vedere Gestione degli avvisi).

- Fare clic su **Log eventi** per visualizzare l'elenco degli eventi per lo chassis selezionato (vedere Monitoraggio degli eventi nel log eventi).
- Fare clic su **Processi** per visualizzare un elenco di processi associati allo chassis (vedere Monitoraggio dei processi).
- Fare clic su **Light Path** per visualizzare lo stato corrente dei LED dello chassis: posizione, errore e informazioni. Questa operazione equivale alla visualizzazione del pannello anteriore dello chassis.
- Fare clic su **Specifiche di alimentazione e termiche** per visualizzare i dettagli relativi all'alimentazione e al flusso d'aria.

  Suggerimento: utilizzare il pulsante di aggiornamento nel browser Web per raccogliere i dati relativi alle specifiche di alimentazione e termiche più recenti. La raccolta dei dati potrebbe richiedere alcuni minuti.
- Fare clic su **Chiavi FoD (Feature on Demand)** per accedere alle informazioni necessarie per ordinare una chiave FoD e altre informazioni senza agenti (vedere Visualizzazione delle chiavi Features on Demand).

Al termine

Oltre a visualizzare il riepilogo e le informazioni dettagliate sullo chassis, è possibile eseguire le seguenti operazioni:

- Visualizzare uno chassis nella vista grafica dello chassis o del rack facendo clic su **Azioni → Viste → Mostra nella vista rack** o **Azioni → Viste → Mostra nella vista chassis**.
- Avviare l'interfaccia Web CMM facendo clic sul collegamento **Indirizzo IP** (vedere Avvio dell'interfaccia Web CMM per uno chassis).
- Modificare le informazioni (ad esempio la descrizione, la posizione e il contatto del Supporto) facendo clic su **Modifica proprietà** (vedere Modifica delle proprietà di sistema per uno chassis).
- Modificare le impostazioni IP di gestione per l'intero chassis, tra cui i nodi di elaborazione e gli switch Flex, facendo clic su **Tutte le azioni → Inventario → Modifica indirizzi IP di gestione** (vedere Modifica delle impostazioni IP di gestione per uno chassis).
- Esportare le informazioni dettagliate sullo chassis in un file CSV facendo clic su **Azioni → Inventario → Esporta inventario**.

  Nota:

  – Per ulteriori informazioni sui dati di inventario nel file CSV, vedere GET /chassis/<*UUID_list*> nella documentazione online di XClarity Administrator.

  – Durante l'importazione di un file CSV in Microsoft Excel, i valori di testo contenenti solo numeri vengono trattati come valori numerici (ad esempio nel caso degli UUID). Impostare la formattazione di ogni cella come testo per risolvere il problema.
- Annullare la gestione di uno chassis (vedere Non gestione di uno chassis).
- Su uno chassis, abilitare o disabilitare le modifiche della regola del firewall che limitano le richieste in entrata solo a quelle provenienti da XClarity Administrator selezionando lo chassis e facendo clic su **Azioni → Sicurezza → Abilita incapsulamento** oppure **Azioni → Sicurezza → Disabilita incapsulamento**.

  L'impostazione globale di incapsulamento è disabilitata per impostazione predefinita. Se disabilitata, la modalità di incapsulamento del dispositivo è impostata su "normale" e le regole del firewall non vengono modificate nell'ambito del processo di gestione.

L'impostazione globale di incapsulamento è disabilitata per impostazione predefinita. Se disabilitata, la modalità di incapsulamento del dispositivo è impostata su "normale" e le regole del firewall non vengono modificate nell'ambito del processo di gestione.

Quando l'impostazione globale di incapsulamento è abilitata e il dispositivo supporta l'incapsulamento, XClarity Administrator comunica con il dispositivo durante il processo di gestione per la modifica della modalità di incapsulamento del dispositivo su "encapsulationLite" e delle regole del firewall sul dispositivo per limitare le richieste in entrata solo a quelle provenienti da XClarity Administrator.

Attenzione: Se l'incapsulamento è abilitato e XClarity Administrator non è più disponibile prima che la gestione di un dispositivo venga annullata, è necessario eseguire la procedura per disabilitare l'incapsulamento al fine di stabilire la comunicazione con il dispositivo. Per le procedure di ripristino, vedere lenovoMgrAlert.mib file e Ripristino della gestione con un modulo CMM dopo un errore del server di gestione.

- Risolvere i problemi che potrebbero verificarsi tra il certificato di sicurezza di XClarity Administrator e quello del modulo CMM nello chassis selezionando uno chassis e facendo clic su **Azioni → Sicurezza → Risolvi certificati non attendibili** (vedere Risoluzione di un certificato server non attendibile).

Backup e ripristino dei dati di configurazione del modulo CMM

Lenovo XClarity Administrator non include funzioni di backup integrate per i dati di configurazione del modulo CMM. Utilizzare le funzioni di backup disponibili per il modulo CMM gestito.

Utilizzare l'interfaccia Web di gestione o l'interfaccia della riga di comando (CLI) per eseguire il backup e il ripristino del modulo CMM.

- Backup dei dati di configurazione del modulo CMM
  - Dall'interfaccia Web di gestione fare clic su **Gestione del modulo di gestione → Configurazione → Configurazione backup**. Per ulteriori informazioni, vedere Salvataggio di una configurazione CMM mediante l'interfaccia Web nella documentazione online di Flex Systems.
  - Dalla CLI utilizzare il comando `write`. Per ulteriori informazioni, vedere Comando CMM write nella documentazione online di Flex Systems.
- Ripristino dei dati di configurazione del modulo CMM
  - Dall'interfaccia Web di gestione fare clic su **Gestione del modulo di gestione → Configurazione → Ripristina configurazione da file**. Per ulteriori informazioni, vedere Ripristino di una configurazione CMM mediante l'interfaccia Web nella documentazione online di Flex Systems.
  - Dall'interfaccia della riga di comando utilizzare il comando `read`. Per ulteriori informazioni, vedere Comando CMM read nella documentazione online di Flex Systems.

Nota: Suggerimento: è possibile trovare informazioni aggiuntive sul backup e il ripristino dei componenti dello chassis in Guida alle procedure ottimali per il backup e il ripristino di PureFlex e Flex System.

Avvio dell'interfaccia Web CMM per uno chassis

È possibile avviare l'interfaccia Web CMM per uno chassis specifico da Lenovo XClarity Administrator.

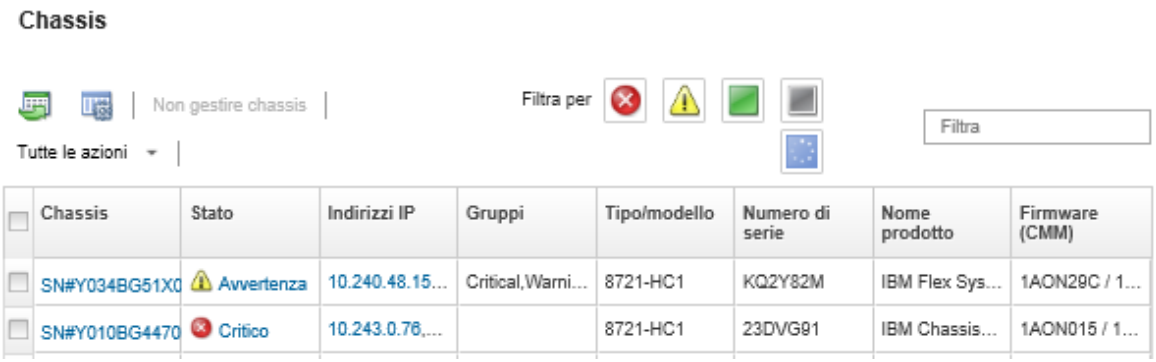
Procedura

Per avviare un'interfaccia Web CMM, attenersi alla procedura descritta di seguito.

Nota: L'avvio di questa interfaccia Web CMM da XClarity Administrator mediante il browser Web Safari non è supporto.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Hardware → Chassis** per visualizzare la pagina Chassis.

È possibile ordinare le colonne della tabella per individuare più facilmente gli chassis che si desidera gestire. Inoltre, è possibile immettere testo (ad esempio, un nome di chassis o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli chassis visualizzati.



Passo 2. Fare clic sul collegamento per lo chassis nella colonna **Chassis**. Verrà visualizzata la relativa pagina di riepilogo dello stato.

Passo 3. Fare clic su **Tutte le azioni → Avvia → Interfaccia Web di gestione**. Verrà avviata l'interfaccia Web CMM.

Suggerimento: è inoltre possibile fare clic sull'indirizzo IP per avviare CMM.

Passo 4. Accedere all'interfaccia Web CMM utilizzando le credenziali utente di XClarity Administrator.

Modifica delle proprietà di sistema per uno chassis

È possibile modificare le proprietà di sistema per uno chassis specifico.

Procedura

Per modificare le proprietà di sistema, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Hardware → Chassis** per visualizzare la pagina Chassis.

Passo 2. Selezionare lo chassis da aggiornare.

Passo 3. Fare clic su **Tutte le azioni → Inventario → Modifica proprietà** per visualizzare la finestra di dialogo Modifica.

Passo 4. Modificare le seguenti informazioni, in base alle esigenze.
- Nome del server
- Contatto supporto
- Descrizione

Nota: Posizione, ambiente, rack e proprietà dell'unità inferiore del rack vengono aggiornati da XClarity Administrator quando si aggiungono o rimuovono dispositivi da un rack nell'interfaccia Web (vedere Gestione dei rack).

Passo 5. Fare clic su **Salva**.

Nota: Quando vengono modificate queste proprietà, è possibile che si verifichi un breve ritardo nella visualizzazione delle modifiche nell'interfaccia Web di XClarity Administrator.

Modifica delle impostazioni IP di gestione per uno chassis

È possibile modificare le impostazioni IP di gestione per l'intero chassis, inclusi nodi di elaborazione, dispositivi di storage e Switch Flex.

Procedura

Per modificare le impostazioni IP di gestione, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Hardware → Chassis** per visualizzare la pagina Chassis.

Passo 2. Selezionare lo chassis.

Passo 3. Fare clic su **Tutte le azioni → Inventario → Modifica indirizzi IP di gestione** per visualizzare la pagina Impostazioni IP componente e chassis.

Passo 4. Modificare le seguenti impostazioni globali, in base alle esigenze.

- Scegliere di abilitare o disabilitare gli indirizzi IPv4.

  Se si abilitano gli indirizzi IPv4, specificare le seguenti impostazioni. Le impostazioni globali IPv4 vengono applicate a un componente quando il suo indirizzo IPv4 è aggiornato.
  - (Facoltativo) Scegliere di ottenere gli indirizzi IP utilizzando gli indirizzi IP assegnati staticamente.
  - Specificare la maschera di sottorete e l'indirizzo gateway.
- Specificare le seguenti impostazioni per gli indirizzi IPv6. Le impostazioni globali IPv6 vengono applicate a un componente quando il suo indirizzo IPv6 è aggiornato.
  - (Facoltativo) Scegliere di ottenere gli indirizzi IP utilizzando gli indirizzi IP assegnati staticamente.

    Se si utilizzano gli indirizzi IP statici, è anche possibile scegliere di utilizzare la configurazione automatica dell'indirizzo IP senza stato e la configurazione dell'indirizzo IP con stato.
  - Specificare la lunghezza del prefisso e l'indirizzo gateway.
- Scegliere se abilitare o disabilitare i server DNS.

  Se si abilitano i server DNS:
  - Scegliere le preferenze di ricerca del server DNS.
  - Immettere gli indirizzi IP da utilizzare per l'ordine di ricerca DNS.
  - Immettere il nome di dominio.

Passo 5. Modificare le seguenti impostazioni IP di CMM.

- Immettere il nome host e l'indirizzo IP per CMM.
- Fare clic su **Genera automaticamente indirizzi IP** per creare indirizzi IP per nodi di elaborazione, dispositivi di storage e Switch Flex utilizzando l'indirizzo IP di CMM come punto di partenza.

Passo 6. Immettere il nome host e gli indirizzi IP per ciascun nodo di elaborazione nello chassis

Passo 7. Immettere il nome host e gli indirizzi IP per ciascun dispositivo di storage nello chassis.

Passo 8. Immettere gli indirizzi IP per ogni Switch Flex nello chassis.

Passo 9. Fare clic su **Salva**. Verrà visualizzata una finestra di dialogo con un riepilogo delle impostazioni di rete.

Passo 10. Fare clic su **Applica**.

Tutti i componenti esistenti nello chassis vengono aggiornati alle impostazioni globali specificate. Una volta completato l'aggiornamento, nella finestra di dialogo verranno visualizzate le impostazioni modificate.

Nota: Quando vengono modificate queste informazioni, è possibile che si verifichi un breve ritardo nella visualizzazione delle informazioni nell'interfaccia di Lenovo XClarity Administrator.

Passo 11. Fare clic su **Chiudi**.

Configurazione del failover di CMM

Quando si installa un secondo CMM in uno chassis, il secondo CMM viene configurato automaticamente come CMM in standby per impostazione predefinita. Se il CMM primario è in stato di errore, l'indirizzo IP del CMM in standby viene modificato nell'indirizzo IP utilizzato per il CMM primario e il CMM in standby assume la gestione dello chassis. Tuttavia, è possibile eseguire una configurazione del failover più avanzata dall'interfaccia Web del controller di gestione per lo chassis.

Informazioni su questa attività

Ad esempio, è possibile scegliere di:

- Disabilitare l'interfaccia di rete per il modulo CMM in standby per impedire il failover.
- Abilitare l'interfaccia di rete per il modulo CMM in standby e consentire lo scambio degli indirizzi IP tra i due CMM durante il failover.
- Abilitare l'interfaccia di rete del modulo CMM in standby e impedire lo scambio degli indirizzi IP tra i due CMM durante il failover.

Per ulteriori informazioni sulle funzionalità di failover avanzate del modulo CMM, vedere Comando advfailover nella documentazione online del modulo CMM.

Procedura

Per abilitare lo scambio di indirizzi IP per i CMM primario e in standby, attenersi alla procedura descritta di seguito.

Passo 1. Dall'interfaccia Web del controller di gestione per lo chassis, fare clic su **Gestione del modulo di gestione → Rete → Ethernet** per visualizzare la pagina Configurazione Ethernet.

Passo 2. Selezionare **IPv4** e **IPv6** per il sistema.

Passo 3. In **Configura indirizzo IP** selezionare l'opzione che consente di utilizzare un indirizzo IP statico. Ripetere l'operazione per l'altro protocollo.

Passo 4. Fare clic su **Gestione del modulo di gestione → Proprietà → Failover avanzato** e abilitare l'opzione di failover avanzato.

Passo 5. Selezionare **Scambia indirizzo IP modulo di gestione**.

Passo 6. Eseguire gli scenari di test per verificare che il failover funzioni correttamente e che Lenovo XClarity Administrator possa connettersi ai moduli CMM primario e di backup.

Riavvio di un modulo CMM

È possibile riavviare un modulo CMM (Chassis Management Module) da Lenovo XClarity Administrator.

Procedura

Completare la seguente procedura per riavviare uno chassis.

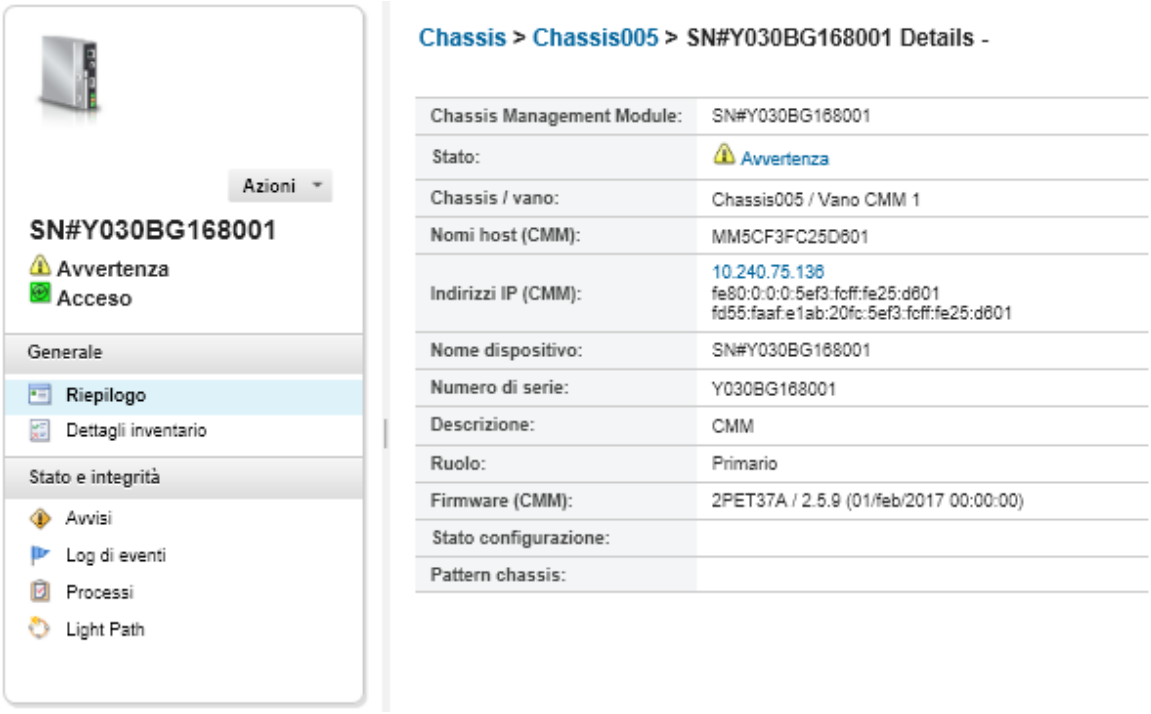
Nota: Quando si riavvia il modulo CMM, tutte le connessioni di rete esistenti sul modulo CMM verranno temporaneamente interrotte.

Passo 1. Dal menu XClarity Administrator, fare clic su **Hardware → Chassis**. Viene visualizzata la pagina Chassis che contiene una vista tabulare di tutti gli chassis gestiti.

Passo 2. Fare clic sul nome dello chassis nella colonna **Chassis** per visualizzare la vista grafica dello chassis.

Passo 3. Fare clic sulla figura del modulo CMM per visualizzare la pagina Riepilogo CMM.

Suggerimento: è inoltre possibile fare clic su **Vista tabella**, quindi sul nome del CMM nella colonna **Nome** per visualizzare la pagina Riepilogo CMM.



Passo 4. Fare clic su **Azioni → Azioni di alimentazione → Riavvia**.

Passo 5. Fare clic su **Riavvia immediatamente**.

Per il completamento di questa operazione potrebbero essere necessari alcuni minuti e potrebbe essere necessario aggiornare la pagina per visualizzare i risultati.

Riposizionamento virtuale di un modulo CMM

È possibile simulare la rimozione e il reinserimento di un modulo CMM (Chassis Management Module) in uno chassis.

Informazioni su questa attività

Durante il riposizionamento virtuale, tutte le connessioni di rete esistenti sul CMM andranno perse e lo stato di alimentazione del CMM verrà modificato.

Attenzione: prima di eseguire un riposizionamento virtuale, verificare di aver salvato tutti i dati utente sul CMM.

Procedura

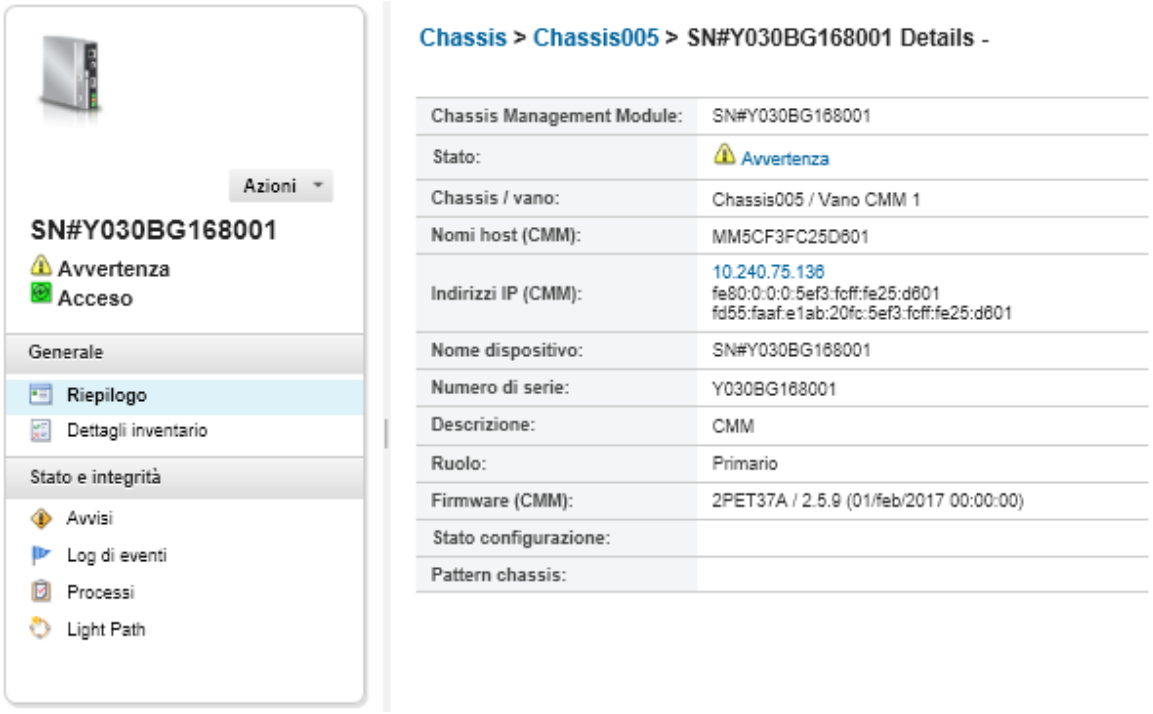
Eseguire le seguenti operazioni per riposizionare virtualmente un modulo CMM.

Passo 1. Dal menu Lenovo XClarity Administrator, fare clic su **Hardware → Chassis**. Viene visualizzata la pagina Chassis che contiene una vista tabulare di tutti gli chassis gestiti.

Passo 2. Fare clic sul nome dello chassis nella colonna **Chassis** per visualizzare la vista grafica dello chassis.

Passo 3. Fare clic sulla figura del modulo CMM per visualizzare la pagina Riepilogo CMM.

Suggerimento: è inoltre possibile fare clic su **Vista tabella**, quindi sul nome del CMM nella colonna **Nome** per visualizzare la pagina Riepilogo CMM.



Passo 4. Fare clic su **Azioni → Servizio → Riposizionamento virtuale**.

Passo 5. Fare clic su **Riposizionamento virtuale**.

Risoluzione di credenziali memorizzate scadute o non valide per uno chassis

Quando una credenziale memorizzata scade o non è più utilizzabili su un dispositivo, lo stato del dispositivo viene visualizzato come "Offline."

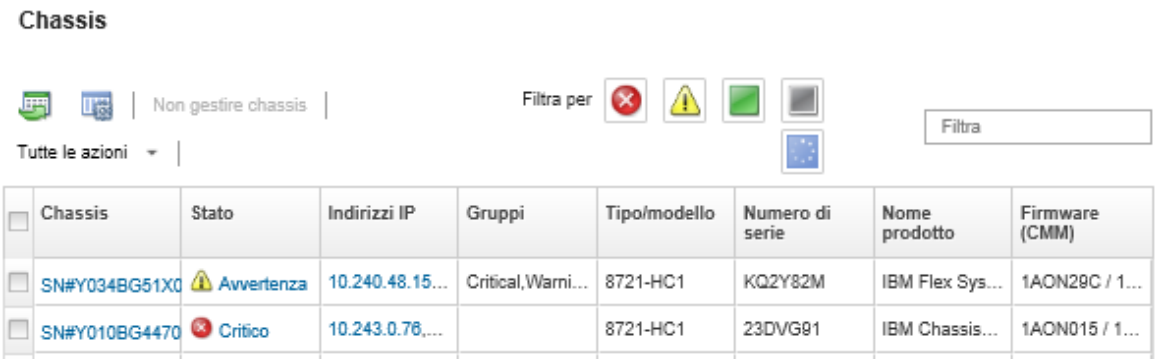
Procedura

Risoluzione di una credenziale memorizzata scaduta o non valida per uno chassis.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware → Chassis**. Viene visualizzata la pagina Chassis che contiene una vista tabulare di tutti gli chassis gestiti.

Passo 2. Fare clic sull'intestazione di colonna **Alimentazione** per raggruppare tutti gli chassis offline nella parte superiore della tabella.

È possibile ordinare le colonne della tabella per individuare più facilmente gli chassis che si desidera gestire. Inoltre, è possibile immettere testo (ad esempio, un nome di chassis o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli chassis visualizzati.



Passo 3. Selezionare lo chassis da risolvere.

Passo 4. Fare clic su **Tutte le azioni → Sicurezza → Modifica credenziali memorizzate**.

Passo 5. Modificare la password per la credenziale memorizzata o selezionare un'altra credenziale memorizzata da utilizzare per il dispositivo gestito.

Nota: Se è stato gestito più di un dispositivo utilizzando le stesse credenziali memorizzate ed è stata modificata la password per le credenziali memorizzate, la modifica della password interessa tutti i dispositivi che attualmente utilizzano le credenziali memorizzate.

Ripristino della gestione con un modulo CMM dopo un errore del server di gestione

Se uno chassis viene gestito da Lenovo XClarity Administrator e XClarity Administrator non funziona, è possibile ripristinare le funzioni di gestione e gli account utente locali per un modulo CMM finché il nodo di gestione non viene ripristinato o sostituito.

Procedura

Completare una delle seguenti procedure per ripristinare la gestione su un modulo CMM.

- Se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID e l'opzione **Forza gestione** (vedere Gestione dello chassis).
- Reimpostare i valori predefiniti di fabbrica del modulo CMM premendo, con l'ausilio di una graffetta, il pulsante a foro stenopeico sul modulo CMM per almeno 10 secondi. Per ulteriori informazioni sul ripristino del modulo CMM, tra cui gli avvisi importanti, vedere Comando CMM Reset nella documentazione online di Flex Systems.
- Reimpostare la configurazione CMM utilizzando la procedura seguente:
  1. Tramite una sessione SSH, aprire un'interfaccia della riga di comando di gestione per lo chassis ed eseguire l'accesso con l'account `RECOVERY_ID`.

     Nota: La password dell'account `RECOVERY_ID` è stata impostata al momento della selezione dello chassis da gestire nella pagina del dominio di gestione. Per ulteriori informazioni sulla gestione degli account centrali, vedere Gestione dello chassis.

     Se si utilizza l'account `RECOVERY_ID` per accedere al CMM per la prima volta sarà necessario modificare la password.
  2. Se richiesto, immettere la nuova password per l'account `RECOVERY_ID`.

3. Ripristinare la configurazione CMM effettuando una delle seguenti operazioni:
   - Se la versione del firmware CMM in esecuzione è quella di giugno 2015 o successive, eseguire il seguente comando:
     `read -f unmanage -T mm[p]`
     Per ulteriori informazioni, consultare la sezione Comando read nella documentazione online del modulo CMM.
   - Se la versione del firmware CMM in esecuzione è precedente a giugno 2015, eseguire i seguenti comandi nell'ordine mostrato:
     a. `env -T mm[p]`
     b. `sslcfg -client disabled -tc1 remove`
     c. `accseccfg -am local`
     d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
     e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
     f. `cimsub -clear all`
     g. `fsmcm -off`

        Il comando `fsmcm` disabilita la gestione degli account utente di XClarity Administrator e consente di utilizzare gli account utente locali con il CMM per eseguire l'autenticazione al CMM e a qualsiasi processore di gestione installato nello chassis.

        Dopo aver eseguito il comando `fsmcm -off`, l'account `RECOVERY_ID` viene rimosso dal registro degli utenti del CMM. La sessione CLI del CMM termina quando si esegue il comando `fsmcm -off`. È ora possibile eseguire l'autenticazione al CMM e agli altri componenti dello chassis utilizzando credenziali CMM locali e utilizzare credenziali CMM locali per accedere all'interfaccia Web CMM o a CLI per lo chassis finché la gestione utenti di XClarity Administrator non viene ripristinata.

        Per ulteriori informazioni, consultare la sezione Comando fsmcm nella documentazione online del modulo CMM.

Una volta ripristinato o sostituito XClarity Administrator, lo chassis potrà essere nuovamente gestito (vedere Gestione dello chassis). Tutte le informazioni sullo chassis (ad esempio le impostazioni di rete) vengono conservate.

Non gestione di uno chassis

È possibile rimuovere uno chassis dalla gestione di Lenovo XClarity Administrator. Questo processo è detto *annullamento della gestione.* Dopo aver annullato la gestione dello chassis, è possibile eseguire l'accesso al modulo CMM per lo chassis utilizzando gli account utente del modulo CMM locale.

Prima di iniziare

È possibile abilitare XClarity Administrator per annullare automaticamente la gestione dei dispositivi che restano offline per un periodo di tempo specifico. Questa opzione è disabilitata per impostazione predefinita. Per abilitare l'annullamento della gestione automatica dei dispositivi offline, fare clic su **Hardware → Rileva e gestisci nuovi dispositivi** dal menu di XClarity Administrator, quindi fare clic su **Modifica** accanto a **Annulla gestione dispositivi offline è Disabilitato**. Quindi, selezionare **Abilita annullamento gestione dispositivi offline** e impostare l'intervallo di tempo. Per impostazione predefinita, i dispositivi non vengono gestiti dopo essere rimasti offline per 24 ore.

Prima di annullare la gestione di uno chassis, verificare che non ci siano processi attivi in esecuzione su qualsiasi dispositivo installato nello chassis.

Se la funzione Call Home è abilitata in XClarity Administrator, Call Home è disabilitata in tutti i server e gli chassis gestiti, al fine di evitare la creazione di record dei problemi duplicati. Se non si intende più utilizzare XClarity Administrator per gestire i dispositivi, sarà possibile riabilitare Call Home in tutti i dispositivi gestiti da XClarity Administrator anziché riabilitare Call Home per ogni singolo dispositivo in un secondo momento (vedere Riabilitazione di call home su tutti i dispositivi gestiti nella documentazione online di XClarity Administrator).

Informazioni su questa attività

Quando si annulla la gestione di uno chassis, XClarity Administrator esegue le seguenti azioni:

- Cancella la configurazione utilizzata per la gestione utenti centralizzata.
- Rimuove il certificato di sicurezza CMM dall'archivio attendibile di XClarity Administrator.
- Se l'opzione Incapsulamento è abilitata sul dispositivo, configura le regole del firewall dei dispositivi con le impostazioni usate prima della gestione del dispositivo.
- Rimuove l'accesso al server NTP dal modulo CMM.
- Rimuove le sottoscrizioni CIM al modulo CMM dalla configurazione di XClarity Administrator in modo che XClarity Administrator non riceva più gli eventi dallo chassis selezionato.

Quando si annulla la gestione di uno chassis, XClarity Administrator conserva alcune informazioni sullo chassis. Queste informazioni vengono riapplicate quando lo stesso chassis viene nuovamente gestito.

Quando si annulla la gestione di uno chassis, gli eventi inviati dai componenti dello chassis vengono ignorati. È possibile conservare questi eventi inoltrando gli eventi a un repository esterno, ad esempio un syslog (vedere Inoltro di eventi).

Suggerimento: tutti i dispositivi dimostrativi aggiunti facoltativamente durante la configurazione iniziale sono nodi di uno chassis. Per annullare la gestione dei dispositivi dimostrativi, annullare la gestione dello chassis mediante l'opzione **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.

Procedura

Per annullare la gestione di uno chassis, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Hardware → Chassis** per visualizzare la pagina Chassis.

Passo 2. Selezionare uno o più chassis dagli elenchi degli chassis gestiti.

Passo 3. Fare clic su **Non gestire chassis**. Viene visualizzata la finestra di dialogo Non gestire.

Passo 4. **Facoltativo:** selezionare **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.

Importante: quando si annulla la gestione di hardware dimostrativo, verificare di aver selezionato questa opzione.

Passo 5. Fare clic su **Non gestire**.La finestra di dialogo Non gestire mostra l'avanzamento di ogni operazione nel processo di annullamento della gestione.

Passo 6. Al termine del processo di annullamento della gestione, fare clic su **OK**.

Al termine

Al termine del processo di annullamento della gestione, sarà possibile eseguire l'accesso al modulo CMM utilizzando gli account utente del CMM locale. Se non si ricordano i nomi utente o le password per gli account utente del CMM locale, reimpostare i valori predefiniti iniziali del modulo CMM per eseguire

l'accesso al CMM. Per informazioni sulla reimpostazione dei valori predefiniti del modulo CMM, vedere Comando CMM Reset nella documentazione online di Flex Systems nella documentazione del prodotto CMM.

Ripristino di uno chassis la cui gestione non è stata annullata correttamente

Se la gestione di uno chassis non è stata annullata correttamente, è necessario ripristinare lo chassis prima di poterne eseguire nuovamente la gestione.

Procedura

Completare una delle seguenti procedure per ripristinare la gestione su un modulo CMM.

- Se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID e l'opzione **Forza gestione** (vedere Gestione dello chassis).
- Reimpostare i valori predefiniti di fabbrica del modulo CMM premendo, con l'ausilio di una graffetta, il pulsante a foro stenopeico sul modulo CMM per almeno 10 secondi. Per ulteriori informazioni sul ripristino del modulo CMM, tra cui gli avvisi importanti, vedere Comando CMM Reset nella documentazione online di Flex Systems.
- Reimpostare la configurazione CMM utilizzando la procedura seguente:
  1. Tramite una sessione SSH, aprire un'interfaccia della riga di comando di gestione per lo chassis ed eseguire l'accesso con l'account `RECOVERY_ID`.

     Nota: La password dell'account `RECOVERY_ID` è stata impostata al momento della selezione dello chassis da gestire nella pagina del dominio di gestione. Per ulteriori informazioni sulla gestione degli account centrali, vedere Gestione dello chassis.

     Se si utilizza l'account `RECOVERY_ID` per accedere al CMM per la prima volta sarà necessario modificare la password.
  2. Se richiesto, immettere la nuova password per l'account `RECOVERY_ID`.
  3. Ripristinare la configurazione CMM effettuando una delle seguenti operazioni:
     - Se la versione del firmware CMM in esecuzione è quella di giugno 2015 o successive, eseguire il seguente comando:
       ```
       read -f unmanage -T mm[p]
       ```
       Per ulteriori informazioni, consultare la sezione Comando read nella documentazione online del modulo CMM.
     - Se la versione del firmware CMM in esecuzione è precedente a giugno 2015, eseguire i seguenti comandi nell'ordine mostrato:
       a. `env -T mm[p]`
       b. `sslcfg -client disabled -tc1 remove`
       c. `accseccfg -am local`
       d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
       e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
       f. `cimsub -clear all`
       g. `fsmcm -off`

          Il comando `fsmcm` disabilita la gestione degli account utente di XClarity Administrator e consente di utilizzare gli account utente locali con il CMM per eseguire l'autenticazione al CMM e a qualsiasi processore di gestione installato nello chassis.

Dopo aver eseguito il comando `fsmcm -off`, l'account `RECOVERY_ID` viene rimosso dal registro degli utenti del CMM. La sessione CLI del CMM termina quando si esegue il comando `fsmcm -off`. È ora possibile eseguire l'autenticazione al CMM e agli altri componenti dello chassis utilizzando credenziali CMM locali e utilizzare credenziali CMM locali per accedere all'interfaccia Web CMM o a CLI per lo chassis finché la gestione utenti di XClarity Administrator non viene ripristinata.

Per ulteriori informazioni, consultare la sezione Comando fsmcm nella documentazione online del modulo CMM.

Una volta ripristinato o sostituito XClarity Administrator, lo chassis potrà essere nuovamente gestito (vedere Gestione dello chassis). Tutte le informazioni sullo chassis (ad esempio le impostazioni di rete) vengono conservate.

Capitolo 8. Gestione dei server

Lenovo XClarity Administrator consente di gestire diversi tipi di sistemi, come i server ThinkAgile, ThinkSystem, Converged, Flex System, NeXtScale, System x® e ThinkServer®.

Ulteriori informazioni:  XClarity Administrator: rilevamento

Prima di iniziare

Nota: I nodi di elaborazione Flex vengono rilevati e gestiti automaticamente quando si gestisce lo chassis che li contiene. Non è possibile rilevare e gestire nodi di elaborazione Flex indipendenti dallo chassis.

Prima di gestire i server, accertarsi di aver soddisfatto le seguenti condizioni:

- Prima di gestire un dispositivo, osservare le relative considerazioni di gestione. Per informazioni, vedere Considerazioni sulla gestione nella documentazione online di XClarity Administrator.
- Alcune porte devono essere disponibili per la comunicazione con i dispositivi. Accertarsi che tutte le porte necessarie siano disponibili prima di gestire i server. Per informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.
- Accertarsi che sia installato il firmware minimo richiesto in ciascun server che si desidera gestire mediante XClarity Administrator. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.
- Accertarsi che nel dispositivo sia abilitato il protocollo CIM over HTTPS.
  1. Eseguire il login all'interfaccia Web di gestione per il server utilizzando l'account utente `RECOVERY_ID`.
  2. Fare clic su **Gestione IMM → Sicurezza**.
  3. Fare clic sulla scheda **CIM su HTTPS** e verificare che **Abilita CIM su HTTPS** sia selezionato.
- Per i server ThinkSystem SR635 e SR655:
  - Verificare che sia installato un sistema operativo e che il server sia stato avviato sul sistema operativo, sul supporto avviabile montato oppure sulla shell EFI almeno una volta, in modo che XClarity Administrator possa raccogliere l'inventario per tali server.
  - Accertarsi che l'opzione IPMI su LAN sia abilitata. L'opzione IPMI su LAN è disabilitata per impostazione predefinita su questi server e deve essere abilitata manualmente prima di poter gestire i server. Per abilitare l'opzione IPMI su LAN mediante TSM, fare clic su **Impostazioni → Configurazione IPMI**. Per rendere effettiva la modifica potrebbe essere necessario riavviare il server.
- Se il certificato del server del dispositivo è firmato da un'autorità di certificazione esterna, accertarsi che il certificato e gli eventuali certificati intermedi vengano importati nell'archivio attendibile di XClarity Administrator (vedere Distribuzione di certificati server personalizzati in dispositivi gestiti).
- Per individuare un server che si trova in una sottorete *differente* da XClarity Administrator, assicurarsi che una delle seguenti condizioni venga soddisfatta:
  - Verificare che sia abilitato l'inoltro SLP multicast sugli switch TOR (Top-of-Rack) e sui router del proprio ambiente. Consultare la documentazione fornita con lo switch o il router specifico per determinare se l'inoltro SLP multicast è abilitato e per reperire le procedure necessarie per abilitarlo qualora sia disabilitato.
  - Se SLP è disabilitato sull'endpoint o nella rete, in alternativa è possibile utilizzare il metodo di rilevamento DNS, aggiungendo manualmente un record di servizio (record SRV) al server DNS (Domain Name Server), ad esempio per XClarity Administrator
    `_lxca._tcp.labs.lenovo.com  service = 0 0 443 fvt-xhmc3.labs.lenovo.com.`

Quindi, abilitare il rilevamento DNS sulla console di gestione della scheda di base dall'interfaccia Web di gestione, facendo clic su **Gestione IMM → Protocollo di rete** e sulla scheda **DNS**, selezionando **Utilizza DNS per rilevare Lenovo XClarity Administrator**.

Nota:

- Il livello di firmware del controller di gestione deve essere aggiornato almeno a maggio 2017 per supportare il rilevamento automatico mediante DNS.
- Se nell'ambiente sono presenti più istanze di XClarity Administrator, il server viene rilevato solo dalla prima istanza che risponde alla richiesta di rilevamento. Il server non viene rilevato da tutte le istanze.

- Per rilevare e gestire i server ThinkServer, accertarsi di aver soddisfatto i seguenti requisiti: Per ulteriori informazioni, vedere Impossibile rilevare un dispositivo e Impossibile gestire un dispositivo nella documentazione online di XClarity Administrator.
  - Il nome host del server deve essere configurato mediante un nome host o un indirizzo IP valido per garantire il rilevamento automatico dei server da parte di XClarity Administrator.
  - La configurazione di rete deve consentire il traffico SLP tra XClarity Administrator e il server.
  - È necessario il protocollo SLP unicast.
  - Per garantire il rilevamento automatico dei server ThinkServer da parte di XClarity Administrator, è richiesto il protocollo SLP multicast. È inoltre necessario abilitare il protocollo SLP in ThinkServer System Manager (TSM).
  - Se i server ThinkServer si trovano su una rete diversa da XClarity Administrator, accertarsi che la rete sia configurata per consentire il protocollo UDP in ingresso attraverso la porta 162, in modo che XClarity Administrator possa ricevere eventi per tali dispositivi.
- Per ThinkAgile, ThinkSystem, Converged, Flex System. NeXtScale e System x, in caso di rimozione, sostituzione o configurazione di eventuali adattatori nel server, riavviare il server almeno una volta per aggiornare le informazioni dei nuovi adattatori nei report del controller di gestione della scheda di base e XClarity Administrator (Accensione e spegnimento di un server).
- In fase di esecuzione di azioni di gestione in un server, accertarsi che quest'ultimo sia spento oppure acceso con avvio alla configurazione BIOS/UEFI o con un sistema operativo in esecuzione. Per eseguire l'avvio alla configurazione BIOS/UEFI dalla pagina Server in XClarity Administrator, fare clic su **Tutte le azioni → Azioni di alimentazione → Riavvia alla configurazione BIOS/UEFI**. Se il server viene avviato senza un sistema operativo, verrà costantemente riavviato dal controller di gestione nel tentativo di rilevarne uno.
- Accertarsi che tutte le impostazioni `UEFI_Ethernet_*` e `UEFI_Slot_*` siano abilitate in Impostazioni uEFI nel server. Per verificare le impostazioni, riavviare il server e, una volta visualizzato il prompt `<F1> Setup`, premere `F1` per avviare Setup Utility. Passare a **System Settings → Devices and I/O ports → Enable/ Disable Adapter Option ROM Support**, quindi individuare la sezione **Enable/Disable UEFI Option ROM (s)** per verificare che le impostazioni siano abilitate.

  Nota: Se supportata, è inoltre possibile utilizzare la funzione Console remota nell'interfaccia del controller di gestione della scheda di base per esaminare e modificare le impostazioni in remoto.
- I server System x3950 X6 devono essere gestiti come due enclosure 4U, ciascuno con il proprio controller di gestione della scheda di base.

Informazioni su questa attività

XClarity Administrator può rilevare automaticamente i server rack e tower in un ambiente individuando i dispositivi gestibili che si trovano nella stessa sottorete IP di XClarity Administrator. Per rilevare i server rack e tower presenti in altre sottoreti, specificare un indirizzo IP o un intervallo di indirizzi IP oppure importare le informazioni da un foglio di calcolo.

Importante: Per i server System x3850 e x3950 X6 è necessario gestire ciascun server nell'ambiente rack scalabile.

Una volta gestiti i server da parte di XClarity Administrator, Lenovo XClarity Administrator esegue periodicamente il polling di ciascun server gestito per raccogliere informazioni, quali inventario, VPD (Vital Product Data) e stato. È possibile visualizzare e monitorare ciascun server gestito ed eseguire azioni di gestione (ad esempio, la configurazione delle impostazioni di sistema, la distribuzione delle immagini del sistema operativo, l'accensione e lo spegnimento).

Per impostazione predefinita, i dispositivi vengono gestiti utilizzando l'autenticazione gestita di XClarity Administrator per eseguire il login ai dispositivi. Quando si gestiscono i server rack e lo chassis Lenovo, è possibile scegliere di utilizzare l'autenticazione locale o gestita per eseguire il login ai dispositivi.

- Quando l'*autenticazione locale* viene utilizzata per i server rack, lo chassis Lenovo e gli switch rack Lenovo, XClarity Administrator utilizza una credenziale memorizzata per eseguire l'autenticazione al dispositivo. La *credenziale memorizzata* può essere un account utente attivo sul dispositivo o un account utente in un server Active Directory.

  Prima di gestire il dispositivo utilizzando l'autenticazione locale è necessario creare le credenziali memorizzate in XClarity Administrator che corrispondono a un account utente attivo sul dispositivo o un account utente in un server Active Directory (vedere Gestione delle credenziali memorizzate nella documentazione online di XClarity Administrator).

  Nota:

  – I dispositivi RackSwitch supportano solo le credenziali memorizzate per l'autenticazione. Le credenziali utente di XClarity Administrator non sono supportate.
- L'*autenticazione gestita* consente di gestire e monitorare più dispositivi utilizzando le credenziali del server di autenticazione XClarity Administrator invece delle credenziali locali. Quando l'autenticazione gestita viene utilizzata per un dispositivo (diverso dai server ThinkServer e System x M4 o dagli switch), XClarity Administrator configura il dispositivo gestito e i relativi componenti installati per utilizzare il server di autenticazione XClarity Administrator per la gestione centralizzata.
  – Quando è abilitata l'autenticazione gestita, è possibile gestire i dispositivi utilizzando le credenziali memorizzate o inserite manualmente (vedere Gestione degli account utente e nella documentazione online di XClarity Administrator).

    La credenziale memorizzata viene utilizzata solo finché XClarity Administrator non configura le impostazioni LDAP sul dispositivo. Successivamente, eventuali modifiche delle credenziali memorizzate non incidono sulla gestione o sul monitoraggio di tale dispositivo.

    Nota: Quando è abilitata l'autenticazione gestita per un dispositivo, non è possibile modificare le credenziali memorizzate per tale dispositivo utilizzando XClarity Administrator.
  – Se viene utilizzato un server LDAP esterno o locale come server di autenticazione XClarity Administrator, gli account utente definiti nel server di autenticazione vengono utilizzati per eseguire il login a XClarity Administrator, CMM e controller di gestione della scheda di base nel dominio di XClarity Administrator. Gli account utente del controller di gestione e CMM locali sono disabilitati.
  – Se viene utilizzato un provider di identità SAML 2.0 come server di autenticazione XClarity Administrator, gli account SAML non saranno accessibili per i dispositivi gestiti. Tuttavia quando si utilizzano un provider di identità SAML e un server LDAP insieme, se il provider di identità utilizza gli account esistenti nel server LDAP, gli account utente LDAP possono essere utilizzati per eseguire il login ai dispositivi gestiti mentre i metodi di autenticazione più avanzati forniti da SAML 2.0 (come autenticazione a più fattori e Single Sign-On) possono essere utilizzati per eseguire il login a XClarity Administrator.
  – La funzione Single Sign-On consente a un utente già connesso a XClarity Administrator di eseguire automaticamente il login al controllo di gestione della scheda di base. L'opzione Single Sign-On è

abilitata per impostazione predefinita quando un server ThinkSystem o ThinkAgile viene inserito nella gestione da XClarity Administrator (a meno che il server non sia gestito con password CyberArk). È possibile configurare l'impostazione globale per abilitare o disabilitare la funzione Single Sign-On per tutti i server ThinkSystem e ThinkAgile gestiti. L'abilitazione dell'opzione Single Sign-On per un server ThinkSystem o ThinkAgile specifico ha la precedenza sull'impostazione globale per tutti i server ThinkSystem e ThinkAgile (vedere).

Nota: Single Sign-On viene disabilitato automaticamente quando si utilizza il sistema di gestione delle identità CyberArk per l'autenticazione.

- Quando l'autenticazione gestita è abilitata per i server ThinkSystem SR635 e SR655:
  - Il firmware del controller di gestione della scheda di base supporta fino a cinque ruoli utente LDAP. XClarity Administrator aggiunge questi ruoli utente LDAP ai server durante la gestione: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** e **lxc-os-admin**.

    È necessario assegnare gli utenti ad almeno uno dei ruoli utente LDAP specificati per comunicare con i server ThinkSystem SR635 e SR655.
  - Il firmware del controller di gestione non supporta gli utenti LDAP con lo stesso nome utente locale del server.
- Per i server ThinkServer e System x M4, il server di autenticazione XClarity Administrator non viene utilizzato. Di contro, viene creato un account IPMI sul dispositivo con il prefisso "LXCA_", seguito da una stringa casuale. (Gli account utente IPMI locali esistenti non vengono disabilitati). Quando si annulla la gestione di un server ThinkServer, l'account utente "LXCA_" viene disabilitato e il prefisso "LXCA_" viene sostituito con il prefisso "DISABLED_". Per determinare se un server ThinkServer è gestito da un'altra istanza, XClarity Administrator verifica gli account IPMI con il prefisso "LXCA_". Se si sceglie di forzare la gestione di un server ThinkServer gestito, tutti gli account IPMI del dispositivo con il prefisso "LXCA_" vengono disabilitati e rinominati. Valutare la possibilità di cancellare manualmente gli account IPMI non più in uso.

  Se si utilizzano credenziali inserite manualmente, XClarity Administrator crea automaticamente una credenziale memorizzata e la utilizza per gestire il dispositivo.

  Nota: Quando è abilitata l'autenticazione gestita per un dispositivo, non è possibile modificare le credenziali memorizzate per tale dispositivo utilizzando XClarity Administrator.

  - Ogni volta che si gestisce un dispositivo utilizzando le credenziali inserite manualmente, viene creata una nuova credenziale memorizzata per tale dispositivo, anche se è stata creata un'altra credenziale memorizzata per il dispositivo durante un processo di gestione precedente.
  - Quando si annulla la gestione di un dispositivo, XClarity Administrator non elimina le credenziali memorizzate create automaticamente per tale dispositivo durante il processo di gestione.

Un dispositivo può essere gestito da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza iniziale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator. Se si verifica un errore durante il processo di annullamento della gestione, sarà possibile selezionare l'opzione **Forza gestione** durante la gestione nella nuova istanza di XClarity Administrator.

Nota: Quando si analizza la rete alla ricerca di dispositivi gestibili, XClarity Administrator non è in grado di sapere se un dispositivo è già gestito da un altro gestore fino a quando non avrà tentato di gestirlo.

Nota: In fase di ricerca di dispositivi gestibili nella rete, XClarity Administrator non rileva se un dispositivo ThinkServer è già gestito; pertanto, i dispositivi ThinkServer gestiti potrebbero apparire nell'elenco dei dispositivi gestibili.

Durante il processo di gestione, XClarity Administrator effettua le azioni seguenti:

- Esegue il login al server utilizzando le credenziali fornite.
- Raccoglie l'inventario per ciascun server.

  Nota: Alcuni dati di inventario vengono raccolti dopo il completamento del processo di gestione. Non sarà possibile eseguire determinate attività su un server gestito (ad esempio, la distribuzione di un pattern server) finché non verranno raccolti tutti i dati di inventario e il server rimarrà nello stato In sospeso.
- Configura le impostazioni per il server NTP in modo che tutti i dispositivi gestiti utilizzino la stessa configurazione di server NTP, impostata su XClarity Administrator.
- Solo server System x e NeXtScale. Assegna i criteri di conformità del firmware più aggiornati al server.
- Solo server Lenovo System x e NeXtScale. Configura facoltativamente le regole del firewall dei dispositivi per consentire di accettare solo le richieste in entrata da XClarity Administrator.
- Solo server System x e NeXtScale. Scambia certificati di sicurezza con il controller di gestione, copiando il certificato server CIM e il certificato client LDAP dal controller di gestione nell'archivio attendibile di XClarity Administrator e inviando il certificato di sicurezza CA e i certificati di attendibilità LDAP di XClarity Administrator al controller di gestione. Il controller di gestione carica i certificati nell'archivio attendibile del controller di gestione, in modo che quest'ultimo possa considerare attendibili le connessioni ai server LDAP e CIM in XClarity Administrator.

  Nota: Se il certificato server CIM o il certificato client LDAP non esiste, verrà creato durante il processo di gestione.
- Configura l'autenticazione gestita, se applicabile. Per ulteriori informazioni sull'autenticazione gestita, vedere Gestione del server di autenticazione.
- Crea l'account utente di ripristino (`RECOVERY_ID`), se applicabile. Per ulteriori informazioni sull'account `RECOVERY_ID`, vedere Gestione del server di autenticazione.

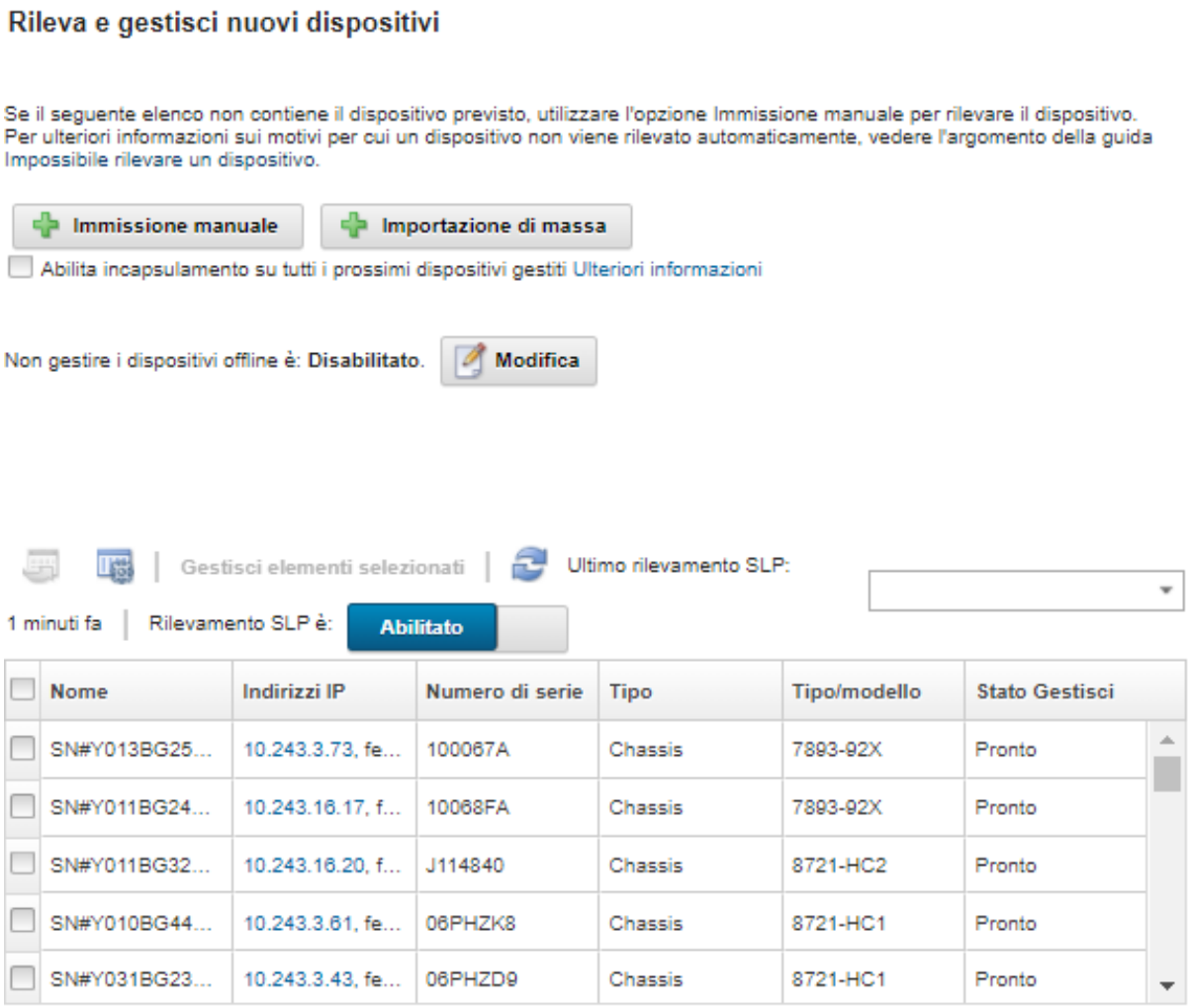
Nota: XClarity Administrator non modifica le impostazioni di sicurezza o crittografiche (la modalità crittografica e la modalità utilizzata per le comunicazioni sicure) durante il processo di gestione. Una volta gestito il server, sarà possibile modificare le impostazioni crittografiche (vedere Configurazione delle impostazioni di crittografia sul server di gestione).

Importante: Se si modifica l'indirizzo IP una volta che il server sarà gestito da XClarity Administrator, XClarity Administrator riconoscerà il nuovo indirizzo IP e continuerà a gestire il server. XClarity Administrator non riconosce tuttavia la modifica dell'indirizzo IP per alcuni server. Se XClarity Administrator indica che il server è offline dopo la modifica dell'indirizzo IP, gestire nuovamente il server mediante l'opzione **Forza gestione**.

Procedura

Per gestire i server rack e tower mediante XClarity Administrator, effettuare una delle seguenti procedure.

- Rilevare e gestire un numero elevato di server rack e tower e altri dispositivi tramite un file di importazione di massa (vedere Gestione dei sistemi nella documentazione online di XClarity Administrator).
- Rilevare e gestire i server rack e tower che si trovano nella stessa sottorete IP di XClarity Administrator.
  1. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci nuovi dispositivi.



È possibile ordinare le colonne della tabella per individuare più facilmente i server che si desidera gestire. È inoltre possibile immettere testo (ad esempio, il nome o l'indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i server visualizzati. È possibile modificare le colonne visualizzate e l'ordinamento predefinito facendo clic sull'icona **Personalizza colonne** ( ).

2. Fare clic sull'icona **Aggiorna** ( ) per rilevare tutti i dispositivi gestibili nel dominio di XClarity Administrator. Il rilevamento potrebbe richiedere diversi minuti.
3. Fare clic sulla casella di controllo **Abilita incapsulamento su tutti i prossimi dispositivi gestiti** per modificare le regole del firewall su tutti i dispositivi durante il processo di gestione affinché le richieste in entrata vengano accettate solo da XClarity Administrator.

   L'incapsulamento può essere abilitato o disabilitato su dispositivi specifici dopo che sono stati gestiti.

   Nota: Quando l'interfaccia di rete di gestione è configurata per utilizzare Dynamic Host Configuration Protocol (DHCP) e quando l'incapsulamento è abilitato, la gestione di un server rack può richiedere molto tempo.

   Attenzione: Se l'incapsulamento è abilitato e XClarity Administrator non è più disponibile prima che la gestione di un dispositivo venga annullata, è necessario eseguire la procedura per disabilitare l'incapsulamento al fine di stabilire la comunicazione con il dispositivo. Per le procedure di ripristino, vedere lenovoMgrAlert.mib file e Ripristino della gestione con un modulo CMM dopo un errore del server di gestione.

4. Selezionare uno o più server che si desidera gestire.
5. Fare clic su **Gestisci elementi selezionati**. Verrà visualizzata la finestra di dialogo Gestisci.
6. Scegliere di utilizzare l'autenticazione gestita o locale di XClarity Administrator per questo dispositivo. L'autenticazione gestita viene selezionata per impostazione predefinita. Per utilizzare l'autenticazione locale, deselezionare **Autenticazione gestita**.
7. Scegliere il tipo di credenziali da utilizzare per autenticare il dispositivo e specificare le credenziali appropriate:
   - **Utilizza credenziali immesse manualmente**
     - Specificare l'ID utente e la password per l'autenticazione con il server.
     - (Facoltativo) Impostare una nuova password per il nome utente specificato, se la password del dispositivo è scaduta.

     Nota: Per utilizzare le credenziali immesse manualmente, è necessario selezionare l'autenticazione gestita di XClarity Administrator.
   - **Utilizza credenziali memorizzate**

     Selezionare la credenziale memorizzata da utilizzare per questo dispositivo gestito. È possibile creare una nuova credenziale memorizzata facendo clic su **Crea nuova**.
   - **Utilizzare il sistema di gestione delle identità esterno**

     Selezionare il sistema di gestione delle identità che si desidera utilizzare per questo dispositivo gestito. Compilare quindi i campi restanti, inclusi l'indirizzo IP o il nome host del server gestito, il nome utente e, facoltativamente, l'ID dell'applicazione, la cartella e la sicurezza.

     Se viene specificato l'ID applicazione, è necessario specificare anche la cartella e la sicurezza, se applicabile.

     Se non viene specificato l'ID dell'applicazione, XClarity Administrator utilizza i percorsi definiti al momento della configurazione di CyberArk per identificare gli account in CyberArk.

     Nota: Sono supportati solo i server ThinkSystem o ThinkAgile. Il sistema di gestione delle identità deve essere configurato in XClarity Administrator, e Lenovo XClarity Controller per i server ThinkSystem o ThinkAgile gestiti deve essere integrato con CyberArk.

   Per gestire il dispositivo si consiglia di utilizzare un account di supervisore o amministratore. Se viene utilizzato un account con autorità di livello inferiore, la gestione potrebbe avere esito negativo oppure potrebbe riuscire ma le altre operazioni XClarity Administrator potrebbero non riuscire sul dispositivo (in particolar modo se il dispositivo viene gestito senza l'autenticazione gestita).

   Per ulteriori informazioni sulle credenziali normali e memorizzate, vedere Gestione degli account utente e Gestione delle credenziali memorizzate.
8. Specificare la password di ripristino, se è selezionata l'autenticazione gestita.

   Quando viene specificata una password, l'account di ripristino (`RECOVERY_ID`) viene creato sul server e tutti gli account utente locali vengono disabilitati. Se si verifica un problema e XClarity Administrator si arresta per qualche motivo, *non* sarà possibile eseguire il login al controller di gestione utilizzando i normali account utente. Tuttavia, è possibile eseguire il login utilizzando l'account di ripristino.

   Nota:

   - La password di ripristino è facoltativa se si sceglie di utilizzare l'autenticazione gestita e non è consentita se si sceglie di utilizzare l'autenticazione locale.
   - È possibile scegliere di utilizzare un account di ripristino locale o le credenziali di ripristino memorizzate. In entrambi i casi, il nome utente è sempre `RECOVERY_ID`.

– Verificare che la password rispetti i criteri di sicurezza e delle password per il dispositivo. I criteri di sicurezza e delle password possono variare.
– Assicurarsi di registrare la password di ripristino per gli usi futuri.
– L'account di ripristino non è supportato per i server ThinkServer e System x M4.

Per ulteriori informazioni sull'ID di ripristino, vedere Gestione del server di autenticazione.

9. Fare clic su **Modifica** per modificare i gruppi di ruoli che devono essere assegnati ai dispositivi.

   Nota:

   – È possibile selezionare un elenco dei gruppi di ruoli assegnati all'utente corrente.
   – Se non si modificano i gruppi di ruoli, vengono utilizzati i gruppi di ruoli predefiniti. Per ulteriori informazioni sui gruppi di ruoli predefiniti, vedere Modifica delle autorizzazioni predefinite.

10. Fare clic su **Gestisci**.

    Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Per garantire il completamento del processo, monitorarne l'avanzamento.

11. Al termine del processo, fare clic su **OK**.

    Il dispositivo è ora gestito da XClarity Administrator, che effettua periodicamente il polling automatico del dispositivo gestito per raccogliere informazioni aggiornate, ad esempio l'inventario.

    Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione **Forza gestione**.

    – Se l'istanza XClarity Administrator di gestione è in errore e non è possibile effettuare il ripristino.

      Nota: se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabile) e l'opzione **Forza gestione**.

    – Se l'istanza XClarity Administrator di gestione è stata disattivata prima di avere annullato la gestione dei dispositivi.
    – Se la gestione dei dispositivi non è stata annullata correttamente.

    Attenzione: I dispositivi possono essere gestiti da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza originale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator.

- Per rilevare e gestire i server rack e tower che non si trovano nella stessa sottorete IP di XClarity Administrator, specificare manualmente gli indirizzi IP.

  1. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci.
  2. Fare clic sulla casella di controllo **Abilita incapsulamento su tutti i prossimi dispositivi gestiti** per modificare le regole del firewall su tutti i dispositivi durante il processo di gestione affinché le richieste in entrata vengano accettate solo da XClarity Administrator.

     L'incapsulamento può essere abilitato o disabilitato su dispositivi specifici dopo che sono stati gestiti.

     Nota: Quando l'interfaccia di rete di gestione è configurata per utilizzare Dynamic Host Configuration Protocol (DHCP) e quando l'incapsulamento è abilitato, la gestione di un server rack può richiedere molto tempo.

     Attenzione: Se l'incapsulamento è abilitato e XClarity Administrator non è più disponibile prima che la gestione di un dispositivo venga annullata, è necessario eseguire la procedura per disabilitare

l'incapsulamento al fine di stabilire la comunicazione con il dispositivo. Per le procedure di ripristino, vedere lenovoMgrAlert.mib file e Ripristino della gestione con un modulo CMM dopo un errore del server di gestione.

3. Selezionare **Immissione manuale**.
4. Specificare gli indirizzi di rete dei server che si desidera gestire:
   - Fare clic su **Singolo sistema** e immettere un singolo nome di dominio dell'indirizzo IP o il nome di dominio completo (FQDN).

     Nota: Per specificare un FQDN, assicurarsi che nella pagina Accesso alla rete sia specificato un nome di dominio valido (vedere Configurazione dell'accesso alla rete).
   - Fare clic su **Più sistemi** e immettere un intervallo indirizzi IP. Per aggiungere un altro intervallo, fare clic sull'icona **Aggiungi** (). Per rimuovere un intervallo, fare clic sull'icona **Rimuovi** ().
5. Fare clic su **OK**. Verrà visualizzata la finestra di dialogo "Gestisci"
6. Scegliere di utilizzare l'autenticazione gestita o locale di XClarity Administrator per questo dispositivo. L'autenticazione gestita viene selezionata per impostazione predefinita. Per utilizzare l'autenticazione locale, deselezionare **Autenticazione gestita**.
7. Scegliere il tipo di credenziali da utilizzare per autenticare il dispositivo e specificare le credenziali appropriate:
   - **Utilizza credenziali immesse manualmente**
     - Specificare l'ID utente e la password per l'autenticazione con il server.
     - (Facoltativo) Impostare una nuova password per il nome utente specificato, se la password del dispositivo è scaduta.

     Nota: Per utilizzare le credenziali immesse manualmente, è necessario selezionare l'autenticazione gestita di XClarity Administrator.
   - **Utilizza credenziali memorizzate**

     Selezionare la credenziale memorizzata da utilizzare per questo dispositivo gestito. È possibile creare una nuova credenziale memorizzata facendo clic su **Crea nuova**.
   - **Utilizzare il sistema di gestione delle identità esterno**

     Selezionare il sistema di gestione delle identità che si desidera utilizzare per questo dispositivo gestito. Compilare quindi i campi restanti, inclusi l'indirizzo IP o il nome host del server gestito, il nome utente e, facoltativamente, l'ID dell'applicazione, la cartella e la sicurezza.

     Se viene specificato l'ID applicazione, è necessario specificare anche la cartella e la sicurezza, se applicabile.

     Se non viene specificato l'ID dell'applicazione, XClarity Administrator utilizza i percorsi definiti al momento della configurazione di CyberArk per identificare gli account in CyberArk.

     Nota: Sono supportati solo i server ThinkSystem o ThinkAgile. Il sistema di gestione delle identità deve essere configurato in XClarity Administrator, e Lenovo XClarity Controller per i server ThinkSystem o ThinkAgile gestiti deve essere integrato con CyberArk.

Per gestire il dispositivo si consiglia di utilizzare un account di supervisore o amministratore. Se viene utilizzato un account con autorità di livello inferiore, la gestione potrebbe avere esito negativo oppure potrebbe riuscire ma le altre operazioni XClarity Administrator potrebbero non riuscire sul dispositivo (in particolar modo se il dispositivo viene gestito senza l'autenticazione gestita).

Per ulteriori informazioni sulle credenziali normali e memorizzate, vedere Gestione degli account utente e Gestione delle credenziali memorizzate.

8. Specificare la password di ripristino, se è selezionata l'autenticazione gestita.

   Quando viene specificata una password, l'account di ripristino (`RECOVERY_ID`) viene creato sul server e tutti gli account utente locali vengono disabilitati. Se si verifica un problema e XClarity Administrator si arresta per qualche motivo, *non* sarà possibile eseguire il login al controller di gestione utilizzando i normali account utente. Tuttavia, è possibile eseguire il login utilizzando l'account di ripristino.

   Nota:

   – La password di ripristino è facoltativa se si sceglie di utilizzare l'autenticazione gestita e non è consentita se si sceglie di utilizzare l'autenticazione locale.
   – È possibile scegliere di utilizzare un account di ripristino locale o le credenziali di ripristino memorizzate. In entrambi i casi, il nome utente è sempre `RECOVERY_ID`.
   – Verificare che la password rispetti i criteri di sicurezza e delle password per il dispositivo. I criteri di sicurezza e delle password possono variare.
   – Assicurarsi di registrare la password di ripristino per gli usi futuri.
   – L'account di ripristino non è supportato per i server ThinkServer e System x M4.

   Per ulteriori informazioni sull'ID di ripristino, vedere Gestione del server di autenticazione.

9. Fare clic su **Modifica** per modificare i gruppi di ruoli che devono essere assegnati ai dispositivi.

   Nota:

   – È possibile selezionare un elenco dei gruppi di ruoli assegnati all'utente corrente.
   – Se non si modificano i gruppi di ruoli, vengono utilizzati i gruppi di ruoli predefiniti. Per ulteriori informazioni sui gruppi di ruoli predefiniti, vedere Modifica delle autorizzazioni predefinite.

10. Fare clic su **Gestisci**.

    Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Per garantire il completamento del processo, monitorarne l'avanzamento.

11. Al termine del processo, fare clic su **OK**.

    Il dispositivo è ora gestito da XClarity Administrator, che effettua periodicamente il polling automatico del dispositivo gestito per raccogliere informazioni aggiornate, ad esempio l'inventario.

    Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione **Forza gestione**.

    – Se l'istanza XClarity Administrator di gestione è in errore e non è possibile effettuare il ripristino.

      Nota: se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabile) e l'opzione **Forza gestione**.

    – Se l'istanza XClarity Administrator di gestione è stata disattivata prima di avere annullato la gestione dei dispositivi.
    – Se la gestione dei dispositivi non è stata annullata correttamente.

    Attenzione: I dispositivi possono essere gestiti da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza originale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator.

Al termine

- Rilevare e gestire dispositivi aggiuntivi.

- Per configurare le informazioni di sistema, lo storage locale, gli adattatori I/O, gli argomenti di avvio le impostazioni del firmware, creare e distribuire pattern server (vedere Configurazione dei server mediante i pattern di configurazione).
- Distribuire le immagini del sistema operativo nei server in cui non ne è installato uno (vedere Installazione dei sistemi operativi sui server bare metal).
- Aggiornare il firmware sui dispositivi non conformi ai criteri correnti (vedere Aggiornamento del firmware sui dispositivi gestiti).
- Aggiungere i dispositivi al rack appropriato per riflettere l'ambiente fisico (vedere Gestione dei rack).
- Monitorare lo stato dell'hardware e i dettagli (vedere Visualizzazione dello stato di un server gestito).
- Monitorare eventi e avvisi (vedere Utilizzo degli eventi e Gestione degli avvisi).
- Cancellare il log SEL di un server facendo clic su **Hardware → Server** dalla barra dei menu di XClarity Administrator, selezionando il server e quindi facendo clic su **Tutte le azioni → Sicurezza → Cancella log SEL**.Questa azione è supportata solo per i server ThinkSystem e ThinkAgile.
- Risolvere le credenziali memorizzate scadute o non valide (vedere Gestione delle credenziali memorizzate).
- Abilitare o disabilitare la funzione Single Sign-On per tutti i server ThinkSystem e ThinkAgile gestiti facendo clic su **Amministrazione → Sicurezza** sulla barra dei menu di XClarity Administrator, facendo clic su **Sessioni attive**, quindi abilitando o disabilitando **Single Sign-On**.
- Disabilitare o abilitare la funzione Single Sign-On per i server ThinkSystem e ThinkAgile gestiti.
  - Per tutti i server ThinkSystem e ThinkAgile gestiti (globalmente), fare clic su **Amministrazione → Sicurezza** sulla barra dei menu di XClarity Administrator, fare clic su **Sessioni attive**, quindi abilitare o disabilitare **Single Sign-On**.
  - Per un server ThinkSystem o ThinkAgile specifico, fare clic su **Hardware → Server** sulla barra dei menu di XClarity Administrator, quindi su **Tutte le azioni → Sicurezza → Abilita Single Sign-On** o **Tutte le azioni → Sicurezza → Disabilita Single Sign-On**.

  Nota: La funzione Single Sign-On consente a un utente già connesso a XClarity Administrator di eseguire automaticamente il login al controllo di gestione della scheda di base. L'opzione Single Sign-On è abilitata per impostazione predefinita quando un server ThinkSystem o ThinkAgile viene inserito nella gestione da XClarity Administrator (a meno che il server non sia gestito con password CyberArk). È possibile configurare l'impostazione globale per abilitare o disabilitare la funzione Single Sign-On per tutti i server ThinkSystem e ThinkAgile gestiti. L'abilitazione dell'opzione Single Sign-On per un server ThinkSystem o ThinkAgile specifico ha la precedenza sull'impostazione globale per tutti i server ThinkSystem e ThinkAgile.

Visualizzazione dello stato di un server gestito

Da Lenovo XClarity Administrator è possibile visualizzare un riepilogo e lo stato dettagliato dei server gestiti e dei relativi componenti installati.

Ulteriori informazioni:

- XClarity Administrator: inventario
- XClarity Administrator: monitoraggio

Informazioni su questa attività

Le seguenti icone di stato vengono utilizzate per indicare l'integrità complessiva del dispositivo. Se i certificati non corrispondono, "(Non attendibile)" viene aggiunto allo stato di ciascun dispositivo applicabile, ad esempio Avvertenza (non attendibile). Se si verifica un problema di connettività o una connessione al

dispositivo non è attendibile, "(Connettività)" viene aggiunto allo stato di ciascun dispositivo applicabile, ad esempio Avvertenza (Connettività).

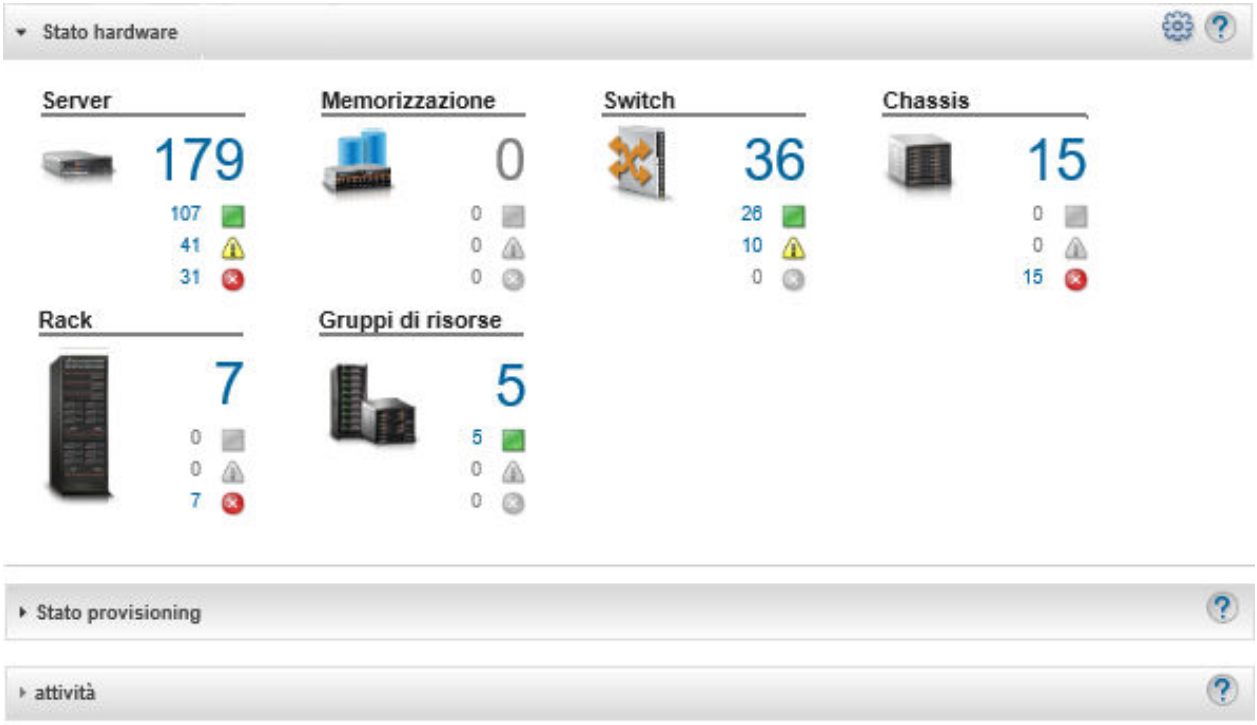
- ( ) Critico
- ( ) Avvertenza
- ( ) In sospeso
- ( ) Informativo
- ( ) Normale
- ( ) Offline
- ( ) Sconosciuto

Un dispositivo può trovarsi in uno dei seguenti stati di alimentazione:
- Attivato
- Disattivato
- Arresto di
- Standby
- Iberna
- Unknown

Procedura

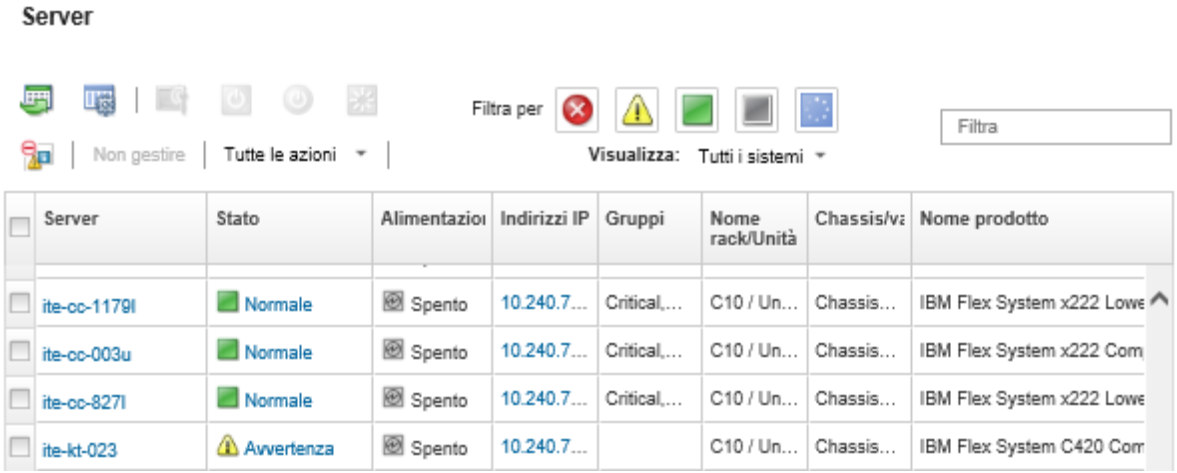
Per visualizzare lo stato di un server gestito, effettuare una o più operazioni tra quelle riportate di seguito.

- Dalla barra dei menu di XClarity Administrator, fare clic su **Dashboard**. Viene visualizzata la pagina Dashboard con una panoramica e lo stato di tutti i dispositivi gestiti e delle altre risorse.



- Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Server**. Verrà visualizzata la pagina Server contenente una vista tabulare di tutti i server gestiti (rack e tower e nodi di elaborazione).

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. Inoltre, è possibile selezionare un tipo di sistema dall'elenco a discesa **Tutti i sistemi**, immettere il testo (come un nome o un indirizzo IP) nel campo **Filtro** e quindi fare clic sulle icone di stato per elencare solo i server che soddisfano i criteri selezionati.



Da questa pagina, è possibile eseguire le seguenti azioni:

- Visualizzare informazioni dettagliate sul server e i relativi componenti (vedere Visualizzazione dei dettagli di un server gestito).
- Visualizzare un server nella vista grafica dello chassis o del rack facendo clic su **Tutte le azioni → Viste → Mostra nella vista rack** o **Tutte le azioni → Viste → Mostra nella vista chassis**.
- Avviare l'interfaccia Web del controller di gestione per il server facendo clic sul collegamento **Indirizzo IP** (vedere Avvio dell'interfaccia del controller di gestione per un server).
- Gestire il server in remoto (vedere Utilizzo del controllo remoto per gestire i server Converged, Flex System, NeXtScale e System x).
- Accendere e spegnere il server (vedere Accensione e spegnimento di un server).
- Per modificare le informazioni di sistema, selezionare un server e fare clic su **Tutte le azioni → Inventario → Modifica proprietà**.
- Per aggiornare l'inventario, selezionare un server e fare clic su **Tutte le azioni → Inventario → Aggiorna inventario**.
- Esportare le informazioni dettagliate su uno o più server in un unico file CSV selezionando il server e facendo clic su **Tutte le azioni → Inventario → Esporta inventario**.

  Nota: è possibile esportare i dati di inventario per un massimo di 60 dispositivi alla volta.

  Suggerimento: Durante l'importazione di un file CSV in Microsoft Excel, i valori di testo contenenti solo numeri vengono trattati come valori numerici (ad esempio nel caso degli UUID). Impostare la formattazione di ogni cella come testo per risolvere il problema.
- Annullare la gestione di un server (vedere Annullamento della gestione di un server rack o tower).
- Reimpostare le impostazioni predefinite di fabbrica degli adattatori di storage locale, facendo clic su **Tutta l'azione → Servizio → Ripristina valori predefiniti per lo storage locale**.
- Per modificare lo stato del LED di posizione in un server su acceso, spento o lampeggiante, selezionare il server e fare clic su **Tutte le azioni → Servizio → Modifica stato LED di posizione**, selezionando lo stato e facendo clic su **Applica**.
  - La commutazione di un LED di posizione per i server ThinkSystem SR635 e SR655 non è supportata.

  - Il LED di posizione nei server ThinkServer può essere acceso o spento. Il lampeggiamento non è supportato.
- Riposizionare virtualmente il server (vedere Riposizionamento virtuale di un server in uno chassis di Flex System).
- Escludere gli eventi che non interessano l'utente da tutte le pagine in cui vengono visualizzati facendo clic sull'icona **Escludi eventi** () (vedere Esclusione di eventi).
- Per riavviare il server tramite NMI (non-maskable interrupt), fare clic su **Tutta l'azione → Servizio → Attiva NMI**.
- In un server, abilitare o disabilitare le modifiche delle regole del firewall che limitano le richieste in entrata solo a quelle provenienti da XClarity Administrator selezionando il server e facendo clic su **Tutte le azioni → Sicurezza → Abilita Incapsulamento** o **Tutte le azioni → Sicurezza → Disabilita Incapsulamento**.L'impostazione globale di incapsulamento è disabilitata per impostazione predefinita. Se disabilitata, la modalità di incapsulamento del dispositivo è impostata su "normale" e le regole del firewall non vengono modificate nell'ambito del processo di gestione.

  Quando l'impostazione globale di incapsulamento è abilitata e il dispositivo supporta l'incapsulamento, XClarity Administrator comunica con il dispositivo durante il processo di gestione per la modifica della modalità di incapsulamento del dispositivo su "encapsulationLite" e delle regole del firewall sul dispositivo per limitare le richieste in entrata solo a quelle provenienti da XClarity Administrator.

  Attenzione: Se l'incapsulamento è abilitato e XClarity Administrator non è più disponibile prima che la gestione di un dispositivo venga annullata, è necessario eseguire la procedura per disabilitare l'incapsulamento al fine di stabilire la comunicazione con il dispositivo. Per le procedure di ripristino, vedere lenovoMgrAlert.mib file e Ripristino della gestione con un modulo CMM dopo un errore del server di gestione.
- (Solo server Converged, Flex System, NeXtScale, System x e ThinkSystem). Per risolvere eventuali problemi tra il certificato di sicurezza di XClarity Administrator e quello del controller di gestione della scheda di base nel server, selezionare un server e fare clic su **Tutte le azioni → Sicurezza → Risolvi certificati non attendibili** (vedere Risoluzione di un certificato server non attendibile).
- Risolvere credenziali memorizzate scadute o non valide per un dispositivo nel gruppo (vedere Risoluzione di credenziali memorizzate scadute o non valide per un server).
- Aggiungere o rimuovere un server da un gruppo di risorse statico facendo clic su **Tutte le azioni → Gruppi → Aggiungi a gruppo** o **Tutte le azioni → Gruppi → Rimuovi da gruppo**.

Visualizzazione dei dettagli di un server gestito

È possibile visualizzare le informazioni dettagliate sui server gestiti da Lenovo XClarity Administrator, tra cui i livelli di firmware, il nome dei server e l'identificatore univoco universale (UUID, Universally Unique Identifier).

Ulteriori informazioni:

-  XClarity Administrator: inventario
-  XClarity Administrator: monitoraggio

Informazioni su questa attività

L'utilizzo della CPU è una misurazione della residenza di stato C aggregata. Viene misurata come percentuale della residenza C0 utilizzata e massima al secondo.

L'utilizzo della memoria è una misurazione dei volumi di lettura/scrittura aggregati di tutti i canali di memoria. Viene calcolata come percentuale della larghezza di banda della memoria utilizzata e massima disponibile al secondo.

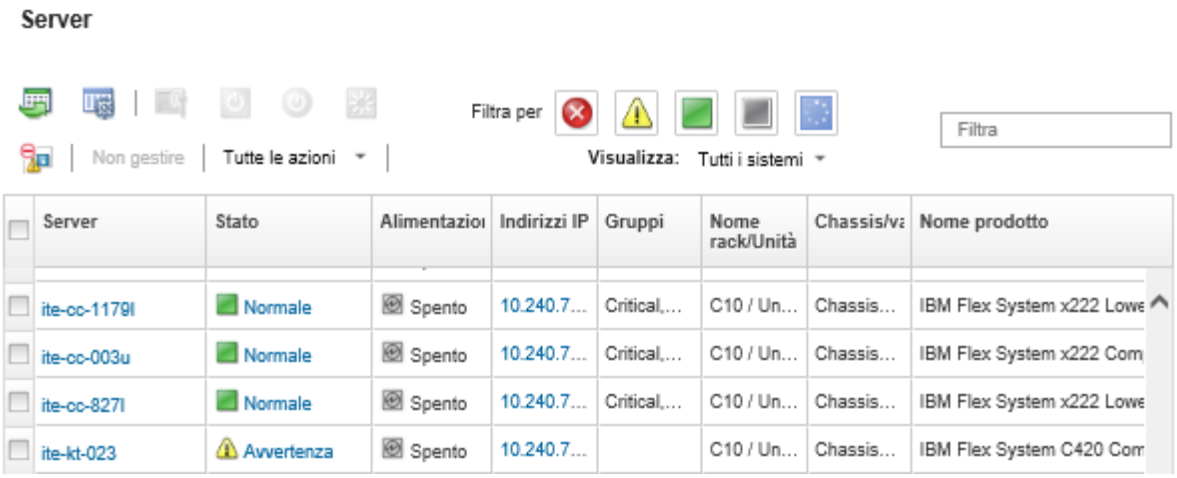
La temperatura dell'aria a livello di sistema viene misurata con un sensore fisico nella parte anteriore del server. Rappresenta la temperatura dell'aria in ingresso del server. La temperatura dell'aria riportata da XClarity Administrator e quella riportata da CMM potrebbero differire se viene acquisita in momenti diversi.

Procedura

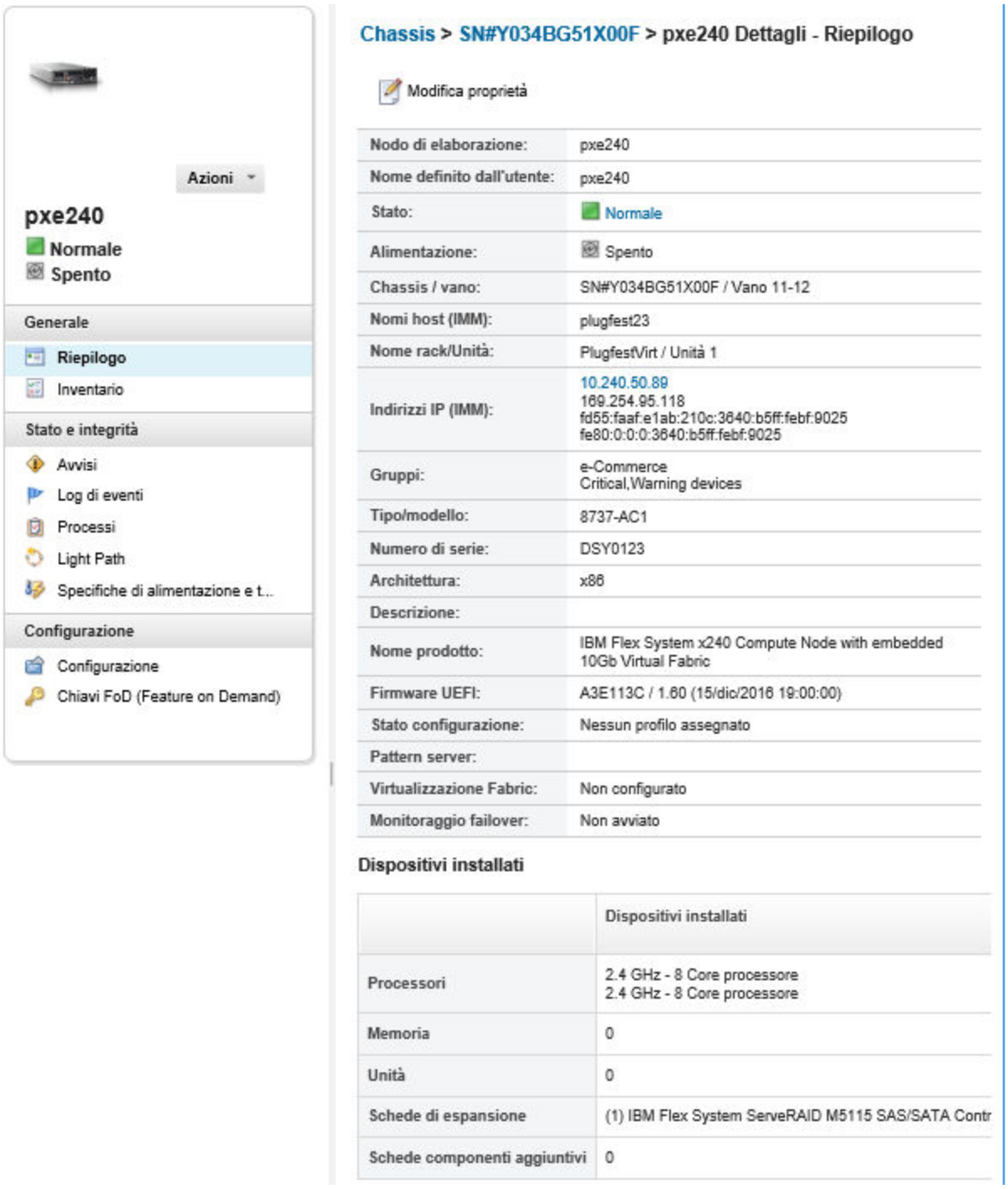
Completare le seguenti operazioni per visualizzare i dettagli per un server gestito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Server**. Viene visualizzata la pagina Server con una vista tabulare di tutti i server gestiti (server rack e nodi di elaborazione).

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. Inoltre, è possibile selezionare un tipo di sistema dall'elenco a discesa **Tutti i sistemi** e immettere testo (ad esempio un nome di sistema o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i server visualizzati.



Passo 2. Fare clic sul collegamento per il server nella colonna **Server**. Viene visualizzata la pagina di riepilogo dello stato del server, che mostra le proprietà del server e un elenco dei componenti installati nel server.



Nota: Per i server System x e NeXtScale, l'indirizzo LAN su USB è elencato in questa pagina; non è tuttavia possibile modificare tale indirizzo da XClarity Administrator. È necessario utilizzare l'interfaccia del controller di gestione della scheda di base per il server. Per ulteriori informazioni, vedere la sezione "Accessing the IMM2 using the LAN over USB interface" nella documentazione relativa al server. La documentazione del server è disponibile nella Documentazione online di BladeCenter.

Passo 3. Completare una o più azioni seguenti:

- Fare clic su **Riepilogo** per visualizzare un riepilogo del server, che include le informazioni di sistema e i componenti installati (vedere Visualizzazione dello stato di un server gestito).

- Fare clic su **Dettagli inventario** per visualizzare i dettagli sui componenti del server, tra cui:
  - Livelli di firmware per il server e il controller di gestione.
  - Dettagli di rete del modulo di gestione, ad esempio il nome host, l'indirizzo IPv4, l'indirizzo IPv6 e gli indirizzi MAC.
  - Dettagli di risorse, tra cui nome server, identificatore univoco universale (UUID) e posizione.
  - Dettagli di componenti, tra cui CPU, memoria, unità e schede di espansione.

  Nota:

  - Sono elencati tutti gli indirizzi IP per il server. L'indirizzo IP per la porta del controller di gestione è la prima voce dell'elenco. Se l'indirizzo IP del controller di gestione è disponibile, viene utilizzato per la connessione al server.
  - Se per uno specifico adattatore non sono disponibili dati, alcuni campi (ad esempio, il nome del prodotto) potrebbero essere vuoti.
  - Se nel server è stato installato un nuovo adattatore, è necessario riavviare il server per visualizzare l'adattatore nell'inventario.
  - Per alcune schede aggiuntive, le informazioni FoD (Feature on Demand) vengono visualizzate sotto il nome del dispositivo.
  - È possibile passare il mouse sui collegamenti nella colonna "Tipo" per ottenere maggiori informazioni su componenti specifici, come la memoria Intel Optain DCPMM.
- Fare clic su **Avvisi** per visualizzare l'elenco di avvisi correnti per il server selezionato (vedere Gestione degli avvisi).

  Nota: È possibile impostare le preferenze delle soglie per la generazione di un avviso e di un evento quando un determinato valore, come la durata di un'unità SSD di un server ThinkSystem o ThinkServer supera un livello di avvertenza o critico (vedere Impostazione delle preferenze delle soglie per la generazione di eventi e avvisi).
- Fare clic su **Log eventi** per visualizzare l'elenco di eventi per il server selezionato (vedere Monitoraggio degli eventi nel log eventi).
- Fare clic su **Processi** per visualizzare un elenco di processi associati al server (vedere Monitoraggio dei processi).
- Fare clic su **light path** per visualizzare lo stato corrente dei LED del server, tra cui posizione, errore e informazioni. Questa operazione equivale alla visualizzazione del pannello anteriore del server.
- Fare clic su **Specifiche di alimentazione e termiche** per visualizzare i dettagli relativi all'utilizzo energetico e alla temperatura dell'aria.

  Suggerimento: utilizzare il pulsante di aggiornamento nel browser Web per raccogliere i dati relativi alle specifiche di alimentazione e termiche più recenti. La raccolta dei dati potrebbe richiedere alcuni minuti.
- Fare clic su **Configurazione** per visualizzare le informazioni di configurazione correnti per il server (inclusi storage locale, adattatori I/O, impostazioni di avvio SAN e impostazioni firmware), oltre alla conformità al pattern di configurazione assegnato (vedere Configurazione dei server mediante i pattern di configurazione).
- Fare clic su **Chiavi FoD (Feature on Demand)** per visualizzare un elenco delle chiavi FoD attualmente installate nel server gestito (vedere Visualizzazione delle chiavi Features on Demand).

Al termine

Oltre a visualizzare il riepilogo e le informazioni dettagliate sul server, procedere come segue:

- Visualizzare il rack o lo chassis associato al server facendo clic sul nome dello chassis o del rack dalla pagina "Riepilogo".
- Visualizzare un server selezionato nella vista grafica dello chassis o del rack facendo clic su **Tutte le azioni → Viste → Mostra nella vista rack** o **Tutte le azioni → Viste → Mostra nella vista chassis**.
- Avviare l'interfaccia Web del controller di gestione per un server selezionato facendo clic sul collegamento **Indirizzo IP** (vedere Avvio dell'interfaccia del controller di gestione per un server).
- Accedere in remoto a un server (vedere Utilizzo del controllo remoto per gestire i server Converged, Flex System, NeXtScale e System x).
- Accendere e spegnere un server selezionato (vedere Accensione e spegnimento di un server).
- Modificare le informazioni di sistema di un server selezionato facendo clic su **Modifica proprietà**.
- Aggiornare l'inventario di un server selezionato facendo clic su **Azioni → Inventario → Aggiorna inventario**.
- Esportare le informazioni dettagliate sui server in un file CSV facendo clic su **Azioni → Inventario → Esporta inventario**.

  Nota:

  – Per ulteriori informazioni sui dati di inventario nel file CSV, vedere GET /nodes/<*UUID_list*> nella documentazione online di XClarity Administrator.

  – Durante l'importazione di un file CSV in Microsoft Excel, i valori di testo contenenti solo numeri vengono trattati come valori numerici (ad esempio nel caso degli UUID). Impostare la formattazione di ogni cella come testo per risolvere il problema.
- Escludere gli eventi che non interessano l'utente da tutte le pagine in cui vengono visualizzati facendo clic su **Azioni → Ripristino servizio → Escludi eventi** (vedere Esclusione di eventi).
- Riavviare un server selezionato tramite NMI (non-maskable interrupt) facendo clic su **Azioni → Servizio → Attiva NMI**.
- Cambiare lo stato del LED di posizione di un server selezionato su acceso, spento o lampeggiante facendo clic su **Azioni → Servizio → Modifica stato LED di posizione**, selezionando lo stato e facendo clic su **Applica**.

  Nota:
  – La commutazione di un LED di posizione per i server ThinkSystem SR635 e SR655 non è supportata.
  – Il LED di posizione nei server ThinkServer può essere acceso o spento. Il lampeggiamento non è supportato.
- Disabilitare o abilitare l'accesso Single Sign-On per un server ThinkSystem o ThinkAgile selezionato facendo clic su **Tutte le azioni → Sicurezza → Abilita Single Sign-On** o **Tutte le azioni → Sicurezza → Disabilita Single Sign-On**.

  La funzione Single Sign-On consente a un utente già connesso a XClarity Administrator di eseguire automaticamente il login al controllo di gestione della scheda di base. L'opzione Single Sign-On è abilitata per impostazione predefinita quando un server ThinkSystem o ThinkAgile viene inserito nella gestione da XClarity Administrator (a meno che il server non sia gestito con password CyberArk). È possibile configurare l'impostazione globale per abilitare o disabilitare la funzione Single Sign-On per tutti i server ThinkSystem e ThinkAgile gestiti. L'abilitazione dell'opzione Single Sign-On per un server ThinkSystem o ThinkAgile specifico ha la precedenza sull'impostazione globale per tutti i server ThinkSystem e ThinkAgile.

  Nota: Single Sign-On viene disabilitato automaticamente quando si utilizza il sistema di gestione delle identità CyberArk per l'autenticazione.
- Abilitare o disabilitare su un server selezionato le modifiche delle regole del firewall che limitano le richieste in entrata solo a quelle provenienti da XClarity Administrator facendo clic su **Azioni → Sicurezza → Abilita incapsulamento** o **Azioni → Sicurezza → Disabilita incapsulamento**. L'impostazione globale

di incapsulamento è disabilitata per impostazione predefinita. Se disabilitata, la modalità di incapsulamento del dispositivo è impostata su "normale" e le regole del firewall non vengono modificate nell'ambito del processo di gestione.

Quando l'impostazione globale di incapsulamento è abilitata e il dispositivo supporta l'incapsulamento, XClarity Administrator comunica con il dispositivo durante il processo di gestione per la modifica della modalità di incapsulamento del dispositivo su "encapsulationLite" e delle regole del firewall sul dispositivo per limitare le richieste in entrata solo a quelle provenienti da XClarity Administrator.

Attenzione: Se l'incapsulamento è abilitato e XClarity Administrator non è più disponibile prima che la gestione di un dispositivo venga annullata, è necessario eseguire la procedura per disabilitare l'incapsulamento al fine di stabilire la comunicazione con il dispositivo. Per le procedure di ripristino, vedere lenovoMgrAlert.mib file e Ripristino della gestione con un modulo CMM dopo un errore del server di gestione.

- (solo server non ThinkServer) Risolvere i problemi che potrebbero verificarsi tra il certificato di sicurezza di Lenovo XClarity Administrator e quello del controller di gestione del server in un server selezionato facendo clic su **Azioni → Sicurezza → Risolvi certificati non attendibili** (vedere Risoluzione di un certificato server non attendibile).

Backup e ripristino dei dati di configurazione del server

Lenovo XClarity Administrator non include funzioni di backup integrate per i dati di configurazione del server. Utilizzare le funzioni di backup disponibili per il server gestito.

- **Server Converged, Flex System, System x, ThinkSystem e NeXtScale**
  - Backup dei dati di configurazione del server

    Utilizzare l'interfaccia Web di gestione o la CLI per eseguire il backup del firmware.

    - Dall'interfaccia Web IMM fare clic su **Gestione IMM → Configurazione IMM**.
    - Dalla CLI utilizzare il comando `backup`.

    Per ulteriori informazioni su come eseguire il backup dei server utilizzando IMM, vedere Documentazione online di Integrated Management Module II.

    Utilizzare gli strumenti forniti dal sistema operativo per il backup delle applicazioni in esecuzione sul server. Per ulteriori informazioni, vedere la documentazione fornita con il sistema operativo.

    Per i dispositivi di elaborazione Flex System assicurarsi di eseguire il backup delle impostazioni per le opzioni installate nei nodi di elaborazione. È possibile eseguire il backup di tutte le impostazioni dei nodi di elaborazione, incluse le impostazioni delle opzioni, utilizzando Advanced Setup Utility (ASU). Per informazioni sull'utilizzo di ASU, vedere Sito Web di Advanced Settings Utility (ASU).
  - Ripristino dei dati di configurazione del server

    Utilizzare l'interfaccia Web di gestione o la CLI per ripristinare il firmware. Per ulteriori informazioni su come ripristinare server utilizzando BMC, vedere Documentazione online di Integrated Management Module II.

    Utilizzare la documentazione fornita con il sistema operativo e le applicazioni in esecuzione sul server per ripristinare il software installato nel server.

    - Dall'interfaccia Web IMM fare clic su **Gestione IMM → Configurazione IMM**.
    - Dall'interfaccia della riga di comando utilizzare il comando `restore`.

Nota: Suggerimento: è possibile trovare informazioni aggiuntive sul backup e il ripristino dei componenti dello chassis in Guida alle procedure ottimali per il backup e il ripristino di PureFlex e Flex System.

- **Server ThinkServer**Le procedure di ripristino variano in base al tipo di server ThinkServer. Per informazioni sul ripristino del dispositivo, consultare la documentazione del prodotto fornita con il server.

Abilitazione di Protezione del sistema

Protezione del sistema monitora le differenze nell'inventario hardware per i server ThinkSystem con XCC2.

Informazioni su questa attività

L'inventario monitorato include processori, memoria, adattatori PCI, unità, scheda di sistema e schede verticali. Non vengono rilevate modifiche ai livelli di firmware e alle impostazioni di configurazione.

Se Protezione del sistema è abilitato, viene eseguita un'istantanea dell'inventario hardware come riferimento attendibile per ciascun dispositivo selezionato. Quando un dispositivo viene riavviato, il controller di gestione della scheda di base nel dispositivo raccoglie la configurazione di sistema corrente e la confronta con l'istantanea. Quando viene rilevata una deviazione per uno o più componenti, Protezione del sistema genera un evento. Se viene rilevata una deviazione per un processore o la memoria, Protezione del sistema genera un evento e, facoltativamente, impedisce l'avvio del server nel sistema operativo.

Procedura

Per abilitare Protezione del sistema su altri server con XCC2, completare le seguenti operazioni.

Passo 1. Dal menu XClarity Administrator, fare clic su **Hardware → Server**. Verrà visualizzata la pagina Server contenente una vista tabulare di tutti i server gestiti.

Passo 2. Selezionare uno o più server con XCC2.

Passo 3. Fare clic su **Tutte le azioni → Sicurezza → Abilita protezione del sistema** per visualizzare la finestra di dialogo Abilita protezione del sistema.

Passo 4. Scegliere l'azione da eseguire quando Protezione del sistema è abilitato, se viene rilevato una modifica dell'inventario e se il server diventa non conforme.

- **Abilita, mantieni comportamento predefinito del sistema**. Viene utilizzato il comportamento corrente. . Il comportamento predefinito è la generazione di un evento.
- **Abilita, impedisci l'avvio del sistema operativo quando non conforme**. Viene generato un evento. Se si tenta di eseguire l'avvio nel sistema operativo, verrà visualizzato un avviso quando Protezione del sistema rileva modifiche della configurazione di processori o memoria. In questo caso, se le modifiche non sono impreviste, verrà richiesto di eseguire l'accesso al controller di gestione della scheda di base. In caso contrario, è possibile continuare il processo di avvio o arresto. Se non si risponde entro 5 minuti, il server viene arrestato per impostazione predefinita.
- **Abilita, genera evento quando non conforme**. Viene generato un evento, ma non vengono eseguite altre azioni.

Passo 5. Fare clic su **Applica**.

Verrà generato un processo per creare istantanee di inventario per il server selezionato. È possibile monitorare l'avanzamento del processo dal log dei processi. Dal menu XClarity Administrator, fare clic su **Monitoraggio → Processi**. Per ulteriori informazioni sul log dei processi, vedere Monitoraggio dei processi.

Al termine

Per disabilitare Protezione del sistema sui server selezionati, fare clic su **Tutte le azioni → Sicurezza → Disabilita protezione del sistema** e selezionare **Applica**.

Cancellazione sicura dei dati dell'unità

Lenovo XClarity Administrator può cancellare in modo sicuro i dati su tutte le unità dei server ThinkSystem e ThinkAgile selezionati in cui sono in esecuzione la versione 22B e quelle successive. Questa operazione riscrive in modo permanente ogni unità, riempendo l'intera unità con uno zero binario, un uno binario o dati casuali, rendendo difficile il rilevamento dei dati precedentemente salvati sull'unità.

Attenzione:

- Questa operazione cancella in modo *permanente* e *irreversibile* tutti i dati sulle unità.
- Non è possibile annullare questa operazione dopo l'invio del processo.

Prima di iniziare

È necessario disporre dell'autorità **lxc-supervisor** per cancellare i dati dell'unità.

Verificare che la password dell'amministratore UEFI non sia impostata nei server gestiti da cancellare. Se la password dell'amministratore UEFI è impostata su un qualsiasi server, le unità in questi server non vengono cancellate.

Per impostazione predefinita, è possibile cancellare in modo sicuro i dati delle unità per un massimo di tre server alla volta. È possibile configurare il numero di server consentiti contemporaneamente facendo clic su **Amministrazione → Preferenze inventario** e impostando il campo **Numero massimo di server che possono essere cancellati in un batch** sul valore desiderato. È possibile scegliere tra `3 - 100` server.

È consentito un solo processo di cancellazione sicura alla volta. È necessario attendere il completamento del processo in corso prima di avviarne un altro sicuro.

La cancellazione di unità di grandi dimensioni potrebbe richiedere diverse ore.

Non è possibile cancellare in modo sicuro i volumi SDD SATA collegati ai controller RAID SATA. Tenere invece in considerazione i consigli che seguono.

- Per le unità SSD SATA da 7 mm, collegarsi ai controller RAID Broadcom per eseguire una cancellazione sicura.
- Per le unità SSD SATA M.2, collegarsi ai controller non RAID Marvell (come il kit di abilitazione a 2 vani SATA/NVMe M.2 per ThinkSystem) per eseguire un'operazione di cancellazione sicura.

Informazioni su questa attività

È possibile cancellare i dati nelle seguenti unità.
- NVMe
- SAS
- HBA SAS
- RAID SAS
- SATA
- Dispositivi di storage collegati esternamente.
  - Lenovo Storage D1212 (MT 4587)
  - Lenovo Storage D1224 (MT 4587)
  - Lenovo Storage D3284 (MT 6413)

L'operazione di cancellazione sicura crea una voce nel log di controllo. È possibile inoltrare questi eventi utilizzando la funzione di inoltro eventi (vedere Inoltro di eventi a syslog, a un programma di gestione SNMP remoto e ad altri servizi di eventi).

Per risolvere i problemi di cancellazione sicura, vedere Impossibile cancellare in modo sicuro i dati dell'unità sulle unità bloccate e Impossibile cancellare in modo sicuro i volumi SDD SATA quando sono collegati a controller RAID Marvell nella documentazione online di XClarity Administrator.

Procedura

Per cancellare in modo sicuro tutte le unità di server gestiti specifici, completare le seguenti operazioni.

Passo 1. Dal menu XClarity Administrator, fare clic su **Hardware → Server**. Verrà visualizzata la pagina Server contenente una vista tabulare di tutti i server gestiti.

Passo 2. Selezionare il server.

Passo 3. Fare clic su **Tutte le azioni → Servizio → Cancellazione sicura dell'unità (HDD/SDD)**.

Passo 4. Immettere la propria password supervisore per confermare che si desidera cancellare tutte le unità nei server selezionati

Passo 5. Fare clic su **Cancella**.

Se si sceglie di eseguire un'operazione di cancellazione dell'unità di massa su più di tre server, verrà richiesto di immettere l'ID utente e la password. Immettere le stesse credenziali utente utilizzate per eseguire l'accesso a XClarity Administrator.

Viene creato un processo per eseguire questa operazione. È possibile monitorare l'avanzamento della pagina Processi, facendo clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator. Se il processo non è stato completato correttamente, fare clic sul relativo collegamento per visualizzare i dettagli sul processo (vedere Monitoraggio dei processi).

Utilizzo di controllo remoto

Dall'interfaccia Web di Lenovo XClarity Administrator è possibile aprire una sessione di controllo remoto a un server gestito, come con una console locale. È possibile utilizzare la sessione di controllo remoto per eseguire operazioni quali accensione o spegnimento del server e montaggio logico di un'unità locale o remota.

Per avviare una sessione di controllo remoto per qualsiasi dispositivo, è necessario disporre dei privilegi **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin** o **lxc-hw-manager**.

Utilizzo del controllo remoto per gestire i server ThinkSystem o ThinkAgile

Dall'interfaccia Web di Lenovo XClarity Administrator è possibile aprire una sessione di controllo remoto a un server ThinkSystem o ThinkAgile gestito, come con una console locale. È possibile utilizzare la sessione di controllo remoto per eseguire operazioni relative all'alimentazione e al montaggio logico di un'unità locale o di rete.

Prima di iniziare

L'incapsulamento deve essere disabilitato sul server.

Per aprire una sessione di controllo remoto su un server, lo stato del server deve essere "Online" o "Normale". Se lo stato di accesso del server è diverso da quelli citati, non è possibile stabilire il collegamento tra la sessione di controllo remoto e il server. Per ulteriori informazioni sulla visualizzazione dello stato dei server, vedere Visualizzazione dei dettagli di un server gestito.

Esaminare le seguenti considerazioni per i server ThinkSystem SR635 e SR655.

- È necessario il firmware del controller di gestione della scheda di base v2.94 o versioni successive.
- È supportata solo la modalità utente multiplo; la modalità utente singolo non è supportata.
- Internet Explorer 11 non è supportato.
- Non è possibile accendere o spegnere un server da una sessione di controllo remoto.

Informazioni su questa attività

È possibile avviare una sessione di controllo remoto per un singolo server ThinkSystem o ThinkAgile da XClarity Administrator.

Per ulteriori informazioni sull'utilizzo della console remota e delle funzioni dei supporti, consultare la documentazione del server ThinkSystem o ThinkAgile.

Nota: Per i server ThinkSystem e ThinkAgile, non è richiesto un ambiente JRE (Java Runtime Environment) con supporto Java WebStart.

Procedura

Per aprire una sessione di controllo remoto su un server specifico, effettuare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Server**. Viene visualizzata la pagina Server con una vista tabulare di tutti i server gestiti (server rack e nodi di elaborazione).

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. Inoltre, è possibile selezionare un tipo di sistema dall'elenco a discesa **Tutti i sistemi** e immettere del testo (come un nome o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i server visualizzati.

Passo 2. Selezionare il server su cui si desidera aprire una sessione di controllo remoto.

Passo 3. Fare clic sull'icona **Controllo remoto** ().

Passo 4. Accettare tutti gli avvisi di sicurezza del browser Web.

Al termine

Se la sessione di controllo remoto non si apre correttamente, vedere Problemi di controllo remoto nella documentazione online di XClarity Administrator.

Utilizzo del controllo remoto per gestire i server ThinkServer e NeXtScale sd350 M5

Dall'interfaccia Web di Lenovo XClarity Administrator, è possibile aprire una sessione di controllo remoto per gestire i server ThinkServer e NeXtScale sd350 M5 come con una console locale. È possibile utilizzare la sessione di controllo remoto per eseguire operazioni di alimentazione e ripristino, montare a livello logico un'unità locale o di rete sul server, acquisire schermate e registrare video.

Prima di iniziare

- Il controllo remoto per questi server richiede un JRE (Java Runtime Environment) con supporto Java WebStart installato lato client. Si consiglia di utilizzare un modulo JDK open source. Se si utilizza JRE o JDK di un fornitore, accertarsi che la licenza sia per utilizzo commerciale. Sono supportati i seguenti JRE.
  - Oracle JRE 7 (vedere Sito Web di download di Oracle Java)

    Attenzione:
    - Java 7 richiede almeno il supporto TLSv1.2 (vedere Configurazione delle impostazioni di crittografia sul server di gestione).
    - Il supporto per Java 7 verrà deprecato in una versione successiva.

  - Oracle JRE 8, che richiede una licenza a pagamento (vedere Sito Web di download di Oracle Java)
  - Adoptium OpenJDK 8 con il plug-in IcedTea-Web v1.8 (vedere Sito Web di Adoptium OpenJDK)
  - Amazon Corretto 8 (vedere Sito Web per il download di Amazon Corretto 8)

  Java WebStart non è incluso nei pacchetti di installazione di OpenJDK o Coretto e deve essere installato separatamente. IcedTea-Web o OpenWebStart può essere utilizzato con la licenza GNU GPLV2 (vedere Sito Web per il download di IcedTea-OpenJDK e Sito Web di OpenWebStart).
- Il controllo remoto richiede l'installazione di una chiave Features on Demand per ThinkServer System Manager Premium Upgrade sui server ThinkServer. Per ulteriori informazioni sulle chiavi FoD installate sui server, vedere Visualizzazione delle chiavi Features on Demand .

Informazioni su questa attività

È possibile avviare una sessione di controllo remoto per un singolo server ThinkServer da XClarity Administrator.

Per aprire una sessione di controllo remoto su un server, lo stato del server deve essere "Online" o "Normale". Se lo stato di accesso del server è diverso da quelli citati, non è possibile stabilire il collegamento tra la sessione di controllo remoto e il server. Per ulteriori informazioni sulla visualizzazione dello stato dei server, vedere Visualizzazione dei dettagli di un server gestito.

Per ulteriori informazioni sull'utilizzo della console remota ThinkServer e delle funzioni dei supporti, consultare la documentazione del server ThinkServer.

Procedura

Per aprire una sessione di controllo remoto su un server specifico, effettuare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Server**. Viene visualizzata la pagina Server con una vista tabulare di tutti i server gestiti (server rack e nodi di elaborazione).

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. Inoltre, è possibile selezionare un tipo di sistema dall'elenco a discesa **Tutti i sistemi** e immettere del testo (come un nome o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i server visualizzati.

Passo 2. Selezionare il server su cui si desidera aprire una sessione di controllo remoto.

Passo 3. Fare clic sull'icona **Controllo remoto** ().

Passo 4. Accettare tutti gli avvisi di sicurezza del browser Web.

Al termine

Se la sessione di controllo remoto non si apre correttamente, vedere Problemi di controllo remoto nella documentazione online di XClarity Administrator.

Utilizzo del controllo remoto per gestire i server Converged, Flex System, NeXtScale e System x

Dall'interfaccia Web di Lenovo XClarity Administrator, è possibile aprire una sessione di controllo remoto per gestire i server Converged, Flex System, NeXtScale e System x come con una console locale.

Prima di iniziare

Ulteriori informazioni:  XClarity Administrator: controllo remoto

- Il controllo remoto per questi server richiede un JRE (Java Runtime Environment) con supporto Java WebStart installato lato client. Si consiglia di utilizzare un modulo JDK open source. Se si utilizza JRE o JDK di un fornitore, accertarsi che la licenza sia per utilizzo commerciale. Sono supportati i seguenti JRE.
  - Oracle JRE 7 (vedere Sito Web di download di Oracle Java)

    Attenzione:
    - Java 7 richiede almeno il supporto TLSv1.2 (vedere Configurazione delle impostazioni di crittografia sul server di gestione).
    - Il supporto per Java 7 verrà deprecato in una versione successiva.
  - Oracle JRE 8, che richiede una licenza a pagamento (vedere Sito Web di download di Oracle Java)
  - Adoptium OpenJDK 8 con il plug-in IcedTea-Web v1.8 (vedere Sito Web di Adoptium OpenJDK)
  - Amazon Corretto 8 (vedere Sito Web per il download di Amazon Corretto 8)

  Java WebStart non è incluso nei pacchetti di installazione di OpenJDK o Coretto e deve essere installato separatamente. IcedTea-Web o OpenWebStart può essere utilizzato con la licenza GNU GPLV2 (vedere Sito Web per il download di IcedTea-OpenJDK e Sito Web di OpenWebStart).
- È possibile avviare una sessione di controllo remoto sui server che eseguono i seguenti sistemi operativi (32 o 64 bit):
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 10
- Il controllo remoto richiede l'installazione di una chiave Features on Demand per la presenza remota sui server Converged, NeXtScale e System x. Quando si visualizza l'elenco di server disponibili, se la chiave FoD non viene rilevata su un server, la sessione di controllo remoto visualizza il messaggio `Chiave di attivazione mancante` per il server. È possibile determinare se la presenza remota è abilitata, disabilitata o non installata su un server dalla pagina Server (vedere Visualizzazione dello stato di un server gestito). Per ulteriori informazioni sulle chiavi FoD installate sui server, vedere Visualizzazione delle chiavi Features on Demand.
- L'account utente utilizzato per avviare la sessione di controllo remoto deve essere un account utente valido definito nel server di autenticazione XClarity Administrator. L'account utente deve disporre di livelli sufficienti di autorizzazione utente per accedere e gestire un server.
- Prima di aprire una sessione di controllo remoto, esaminare le considerazioni relative a sicurezza, prestazioni e tastiera. Per ulteriori informazioni su queste considerazioni, vedere Considerazioni sul controllo remoto.
- La finestra di dialogo di controllo remoto utilizza le impostazioni internazionali e della lingua di visualizzazione definite per il sistema operativo sul sistema locale.Se sul sistema locale è in esecuzione Windows, vedere il Sito Web di Java per informazioni su come modificare l'impostazione locale. Per modificare la lingua di visualizzazione, installare una copia localizzata di Windows o un Language Pack dal Sito Web di Windows.

Informazioni su questa attività

È possibile avviare più sessioni di controllo remoto da Lenovo XClarity Administrator. Ogni sessione può gestire più server.

Per aprire una sessione di controllo remoto su un server, lo stato del server deve essere "Online" o "Normale". Se lo stato di accesso del server è diverso da quelli citati, non è possibile stabilire il collegamento tra la sessione di controllo remoto e il server. Per ulteriori informazioni sulla visualizzazione dello stato dei server, vedere Visualizzazione dei dettagli di un server gestito.

È possibile aprire una sessione di controllo remoto non assegnata facendo clic su **Provisioning → Controllo remoto** sulla barra dei menu di Lenovo XClarity Administrator. Quindi, accettare tutti gli avvisi di sicurezza del browser Web.

Nota: Per i nodi di elaborazione Flex System x280, x480 e x880, è possibile avviare una sessione di controllo remoto solo per il nodo primario. Se si tenta di avviare una sessione di controllo remoto per un nodo non primario in un sistema multinodo, la finestra di dialogo di controllo remoto si avvia ma non viene visualizzato alcun video.

Procedura

Completare le seguenti operazioni per aprire una sessione di controllo remoto su un server specifico Converged, Flex System, NeXtScale e System x.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Server**. Viene visualizzata la pagina Server con una vista tabulare di tutti i server gestiti (server rack e nodi di elaborazione).

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. Inoltre, è possibile selezionare un tipo di sistema dall'elenco a discesa **Tutti i sistemi** e immettere del testo (come un nome o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i server visualizzati.

Passo 2. Selezionare il server su cui si desidera aprire una sessione di controllo remoto.

Passo 3. Fare clic sull'icona **Controllo remoto** ().

Passo 4. Accettare tutti gli avvisi di sicurezza del browser Web.

Passo 5. Facoltativamente, salvare l'icona di controllo remoto sul desktop. È possibile utilizzare questa icona per avviare una sessione di controllo remoto senza accedere all'interfaccia Web di XClarity Administrator.

Passo 6. Quando richiesto, selezionare una delle seguenti modalità di connessione:

- **Modalità utente singolo**. Stabilisce una sessione di controllo remoto esclusiva con il server. Tutte le altre sessioni di controllo remoto a questo server sono bloccate fino alla disconnessione dal server. Questa opzione è disponibile solo se non sono presenti altre sessioni di controllo remoto al server.
- **Modalità multiutente**. Consente di stabilire più sessioni di controllo remoto con lo stesso server. XClarity Administrator supporta fino a sei sessioni di controllo remoto simultanee a un singolo server.

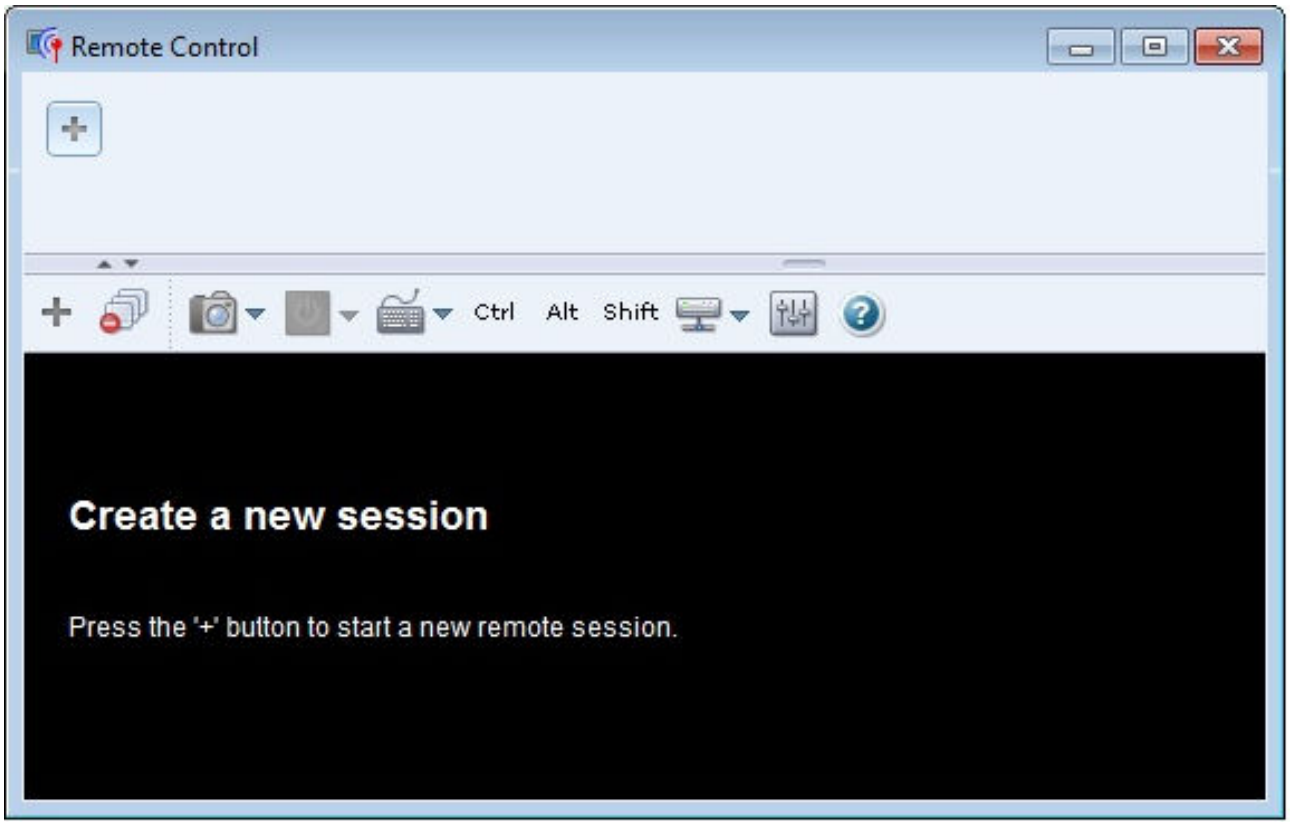
Passo 7. Quando richiesto, scegliere la posizione dove salvare un collegamento alla sessione di controllo remoto sul sistema locale.

Se si salva il collegamento, è possibile utilizzarlo per aprire una sessione di controllo remoto al server specificato senza doverla avviare dall'interfaccia Web di XClarity Administrator. Tuttavia, il sistema locale deve avere accesso a XClarity Administrator per convalidare l'account utente con il server di autenticazione XClarity Administrator.

Il collegamento contiene un link che apre una sessione di controllo remoto vuota, a cui è possibile aggiungere manualmente i server.

Risultati

Viene visualizzata la finestra Controllo remoto.



Nell'area miniature vengono visualizzate le miniature di tutte le sessioni dei server attualmente gestite tramite la sessione di controllo remoto.

È possibile visualizzare più sessioni dei server e spostarsi tra le sessioni dei server facendo clic su una miniatura, in cui viene visualizzata la console del server nell'area delle sessioni video. Se si accede a più server rispetto al numero massimo visualizzabile nell'area miniature, fare clic sull'icona **Scorri a destra** ( ) e sull'icona **Scorri a sinistra** ( ) per scorrere le miniature aggiuntive dei server. Fare clic sull'icona **Tutte le sessioni** ( ) per visualizzare un elenco di tutte le sessioni server aperte.

Dall'area miniature, fare clic sull'icona **Aggiungi server** ( ) per aggiungere un nuovo server all'elenco di server che si sta gestendo. Per ulteriori informazioni sull'aggiunta di una sessione, vedere Aggiunta di una console del server alla sessione di controllo remoto. Dalla pagina "Miniature" è possibile decidere se visualizzare l'area miniature e la frequenza di aggiornamento delle miniature. Per ulteriori informazioni sulle impostazioni delle miniature, vedere Impostazione delle preferenze di controllo remoto.

Al termine

Se la sessione di controllo remoto non si apre correttamente, vedere Problemi di controllo remoto nella documentazione online di XClarity Administrator.

Dalla finestra di dialogo "Controllo remoto", è possibile eseguire le seguenti operazioni:

- Aggiungere una sessione ad altri server alla sessione di controllo remoto corrente (vedere Aggiunta di una console del server alla sessione di controllo remoto).
- Nascondere o mostrare l'area miniature facendo clic sull'icona **Attiva/Disattiva miniature** ( ).

- Visualizzare la sessione di controllo remoto in finestra o a schermo intero facendo clic sull'icona **Schermo** () e quindi su **Attiva schermo intero** o **Disattiva schermo intero**.
- Utilizzare i tasti Ctrl, Alt e Maiusc in una sessione di controllo remoto (vedere Utilizzo dei tasti Ctrl, Alt e Maiusc).
- Definire sequenze di tasti personalizzate, note come softkey (vedere Definizione di tasti softkey).
- Effettuare una cattura della schermata della sessione del server attualmente selezionato e salvarla in vari formati, facendo clic sull'icona **Schermo** () e quindi su **Screenshot**.
- Montare supporti remoti (come CD, DVD o dispositivi USB, immagini disco o ISO) sul server selezionato oppure spostare un dispositivo montato su un altro server (vedere Montaggio o spostamento di supporti remoti).
- Caricare le immagini su un server dai supporti remoti (vedere Caricamento di un'immagine sul server).
- Accendere o spegnere il server da una console remota (vedere Accensione e spegnimento di un server da una sessione di controllo remoto).
- Modificare le preferenze di controllo remoto (vedere Impostazione delle preferenze di controllo remoto).

Considerazioni sul controllo remoto

Esaminare le considerazioni su sicurezza, prestazioni e tastiera relative all'accesso ai server gestiti tramite una sessione di controllo remoto.

Considerazioni sulla sicurezza

L'account utente utilizzato per avviare la sessione di controllo remoto deve essere un account utente valido definito nel server di autenticazione Lenovo XClarity Administrator. L'account utente deve disporre di livelli sufficienti di autorizzazione utente per accedere e gestire un server.

Per impostazione predefinita, è possibile stabilire sessioni di controllo remoto a un server. Tuttavia, quando si avvia una sessione di controllo remoto, è possibile avviare la sessione in modalità utente singolo, che stabilisce una sessione esclusiva con il server. Tutte le altre sessioni di controllo remoto a questo server sono bloccate fino alla disconnessione dal server.

Nota: Questa opzione è disponibile solo se al momento non sono presenti altre sessioni di controllo remoto al server.

Per utilizzare lo standard FIPS (Federal Information Processing Standard) 140, è necessario abilitarlo manualmente completando le seguenti operazioni sul sistema locale:

1. Individuare il nome del fornitore del sistema di crittografia certificato FIPS 140 installato sul sistema locale.

   Suggerimento: per ulteriori informazioni sulla conformità FIPS 140, vedere Sito Web della conformità FIPS 140 di SunJSSE.
2. Modificare il file `$(java.home)/lib/security/java.security`.
3. Modificare la riga che include `com.sun.net.ssl.internal.ssl.Provider` aggiungendo il nome del fornitore del sistema di crittografia certificato FIPS 140. Ad esempio, modificare:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider`
   in:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS`

Considerazioni sulle prestazioni

Se una sessione di controllo remoto è lenta o bloccata, chiudere tutti i video e le sessioni dei supporti remoti stabilite con il server selezionato per ridurre il numero di connessioni aperte con il server. Inoltre, è possibile

aumentare le prestazioni modificando le seguenti preferenze. Per ulteriori informazioni, vedere Impostazione delle preferenze di controllo remoto.

- **KVM**
  - Ridurre la percentuale della larghezza di banda video utilizzata dall'applicazione. La qualità delle immagini della sessione di controllo remoto verrà ridotta.
  - Ridurre la percentuale dei frame aggiornati dall'applicazione. La velocità di aggiornamento della sessione di controllo remoto verrà ridotta.
- **Miniature**
  - Aumentare la velocità dell'intervallo di aggiornamento delle miniature. L'applicazione aggiornerà le miniature a una velocità inferiore.
  - Disattivare completamente la visualizzazione delle miniature.

La dimensione della finestra della sessione di controllo remoto e il numero di sessioni attive potrebbero incidere sull'utilizzo delle risorse della workstation, come memoria e larghezza di banda della rete, riducendo le prestazioni. La sessione di controllo remoto utilizza un limite flessibile di 32 sessioni aperte. Se vengono aperte più di 32 sessioni, le prestazioni potrebbero essere notevolmente ridotte e la sessione di controllo remoto potrebbe bloccarsi. È possibile visualizzare la riduzione delle prestazioni con meno di 32 sessioni aperte, se le risorse, come larghezza di banda della rete e memoria locale, non sono sufficienti.

Considerazioni sulla tastiera

La sessione di controllo remoto supporta i seguenti tipi di tastiera:
- Belga a 105 tasti
- Brasiliano
- Cinese
- Francese a 105 tasti
- Tedesco a 105 tasti
- Italiano a 105 tasti
- Giapponese a 109 tasti
- Coreano
- Portoghese
- Russo
- Spagnolo a 105 tasti
- Svizzero a 105 tasti
- Regno Unito a 105 tasti
- Stati Uniti a 104 tasti

Per informazioni sulle preferenze delle tastiere, vedere Impostazione delle preferenze di controllo remoto.

Aggiunta di una console del server alla sessione di controllo remoto

È possibile aggiungere una o più console del server alla sessione di controllo remoto corrente.

Procedura

Per aggiungere una o più console del server alla sessione di controllo remoto corrente, completare le seguenti operazioni.

Passo 1. Dalla finestra Controllo remoto, fare clic sull'icona **Nuova sessione** ().

Viene visualizzata una finestra di dialogo con un elenco di chassis e server rack disponibili gestiti da Lenovo XClarity Administrator, per i quali l'account utente dispone delle autorizzazioni di gestione.

Suggerimento: se nell'elenco non viene visualizzato alcun server, vedere Problemi di controllo remoto nella documentazione online di XClarity Administrator per le procedure di risoluzione del problema.

Passo 2. Selezionare uno o più server ai quali si desidera collegarsi.

È possibile filtrare i server visualizzati, selezionando un tipo di sistema dall'elenco a discesa **Tipo** e immettendo del testo (ad esempio un nome di sistema o di un enclosure) nel campo **Filtro**.

È possibile selezionare **Seleziona tutto** per selezionare tutti i server nell'elenco.

Passo 3. **Facoltativo:** selezionare **Modalità utente singolo** per aprire una sessione esclusiva per ogni server selezionato.

Se si seleziona questa opzione, tutte le altre sessioni di controllo remoto dei server selezionati vengono bloccate fino alla disconnessione dai server selezionati. Questa opzione è disponibile solo se non sono presenti altre sessioni di controllo remoto dei server selezionati.

Se non si seleziona questa opzione, la modalità multiutente viene utilizzata per impostazione predefinita.

Passo 4. Fare clic su **Connetti**.

Accensione e spegnimento di un server da una sessione di controllo remoto

È possibile accendere e spegnere un server da una sessione di controllo remoto.

Procedura

Per accendere e spegnere un server, completare la seguente procedura.

Passo 1. Dalla finestra Controllo remoto, fare clic sulla miniatura del server che si desidera accendere o spegnere.

Passo 2. Fare clic sull'icona **Alimentazione** (), quindi fare clic su una delle seguenti azioni di alimentazione:

- **Accendi**
- **Spegni normalmente**
- **Spegni immediatamente**
- **Riavvia normalmente**
- **Riavvia immediatamente**
- **Attiva NMI**
- **Riavvia con la configurazione di sistema** (solo server Lenovo Converged, Flex System, NeXtScale e System x)

Suggerimento: l'icona **Alimentazione** è verde se il server è acceso.

Definizione di tasti softkey

È possibile definire sequenze di tasti personalizzate, denominate *softkey, per la sessione di controllo remoto corrente.*

Prima di iniziare

Per visualizzare l'elenco corrente di definizioni di softkey, fare clic sull'icona **Tastiera** ().

Le definizioni di softkey sono memorizzate nel sistema da cui è stata avviata la sessione di controllo remoto. Pertanto, se si avvia la sessione di controllo remoto da un altro sistema, è necessario definire nuovamente i tasti softkey.

È possibile scegliere di esportare le impostazioni utente (che includono i tasti softkey) dalla scheda **Impostazioni utente** nella finestra di dialogo Preferenze. Per ulteriori informazioni, vedere Importazione ed esportazione delle impostazioni utente.

Nota: Se si utilizza una tastiera internazionale e vengono definiti tasti softkey che richiedono l'utilizzo del tasto AltGr (Alternate Graphics), verificare che il sistema operativo della workstation usata per richiamare l'applicazione di controllo remoto sia dello stesso tipo di quello del server a cui si accede in remoto. Ad esempio, se sul server è in esecuzione Linux, assicurarsi di richiamare la sessione di controllo remoto da una workstation Linux.

Procedura

Per aggiungere un tasto softkey, completare la seguente procedura.

Passo 1. Dalla finestra Controllo remoto, fare clic sull'icona **Tastiera** (), quindi fare clic su **Aggiungi softkey**. Viene visualizzata la scheda **Programmazione softkey** nella finestra di dialogo Preferenza.

Passo 2. Fare clic su **Nuovo**.

Passo 3. Immettere la sequenza di tasti che si desidera definire.

Passo 4. Fare clic su **OK**. La nuova softkey viene aggiunta all'elenco di softkey.

Utilizzo dei tasti Ctrl, Alt e Maiusc

Alcuni sistemi operativi intercettano determinati tasti invece di inviarli al server remoto. È possibile utilizzare i pulsanti permanenti per inviare la sequenza tasti direttamente al server che si sta gestendo.

Procedura

Per inviare le combinazioni di tasti Ctrl o Alt, fare clic su **Ctrl** o **Alt** nella barra degli strumenti, posizionare il cursore nell'area delle sessioni video e premere un tasto sulla tastiera.

Ad esempio, per inviare una combinazione di tasti Ctrl+Alt+Canc, effettuare le seguenti operazioni:

1. Fare clic su **Ctrl** nella barra degli strumenti.
2. Fare clic su **Alt** nella barra degli strumenti.
3. Fare clic con il pulsante sinistro del mouse su un punto qualsiasi nell'area delle sessioni video.
4. Premere il tasto Canc sulla tastiera.

Nota: Se viene abilitata la modalità di acquisizione mouse, premere il tasto Alt sinistro per spostare il cursore all'esterno dell'area delle sessioni video. Anche se la modalità di acquisizione mouse è disabilitata per impostazione predefinita, è possibile abilitarla dalla pagina della barra degli strumenti (vedere Impostazione delle preferenze di controllo remoto).

Quando per attivare la chiave si fa clic su **Ctrl**, **Alt** o **Maiusc** nella barra degli strumenti, la chiave resta attiva finché non viene premuto nuovamente un tasto della tastiera o del mouse.

Montaggio o spostamento di supporti remoti

È possibile utilizzare la funzione dei supporti remoti per montare i supporti remoti (come CD, DVD, dispositivi USB, immagini disco o ISO) presenti sul sistema locale nel server selezionato. È inoltre possibile caricare un'immagine nello storage locale disponibile sul controller di gestione della scheda di base.

Prima di iniziare

Solo un utente per volta può montare e caricare i dati nello storage locale del controller di gestione. Durante il montaggio o il caricamento dei dati nello storage locale, agli altri utenti viene impedito l'accesso allo storage locale del controller di gestione.

Su un server su cui è in esecuzione il sistema operativo Linux, il montaggio di più immagini ISO non è supportato.

Procedura

Per montare o spostare i supporti remoti, completare le seguenti operazioni.

Passo 1. Dalla finestra Controllo remoto, fare clic sull'icona **Supporti remoti** ( ).

Passo 2. Fare clic su una delle seguenti azioni:

- **Monta supporti remoti**

  Questa azione rende disponibili le risorse dei supporti locali sul server attualmente selezionato. Una risorsa del supporto può essere montata solo su un server per volta, nell'ambito di una singola sessione di controllo remoto.

  Quando si fa clic su **Monta supporti remoti**, sono disponibili le seguenti opzioni:

  – **Seleziona un'immagine da montare**. L'immagine è disponibile sul server attualmente selezionato finché il dispositivo non viene smontato o la sessione di controllo remoto non viene chiusa. È possibile montare più immagini su un unico server e ogni immagine può essere montata su più server.

  – **Selezionare un'unità, come CD, DVD o dispositivo USB, da montare**. Il dispositivo è disponibile sul server attualmente selezionato finché l'unità non viene smontata o la sessione di controllo remoto non viene chiusa. È possibile montare più dispositivi su un unico server, ma ogni dispositivo può essere montato solo su un server alla volta.

    Nota: Se si seleziona un'unità, accertarsi di smontare l'unità prima di rimuovere i supporti dall'unità.

  – **Carica l'immagine su IMM**. Utilizzare questa opzione per archiviare un'immagine nello storage locale del controller di gestione del server selezionato. L'immagine resta nel controller di gestione anche se la sessione di controllo remoto viene terminata o il server viene riavviato.

    Nel controller di gestione è possibile archiviare circa 50 MB di dati.

    È possibile caricare più immagini nel controller di gestione, a condizione che lo spazio totale utilizzato per tutte le immagini sia inferiore a 50 MB.

    Ogni immagine che viene caricata nel controller di gestione viene montata automaticamente sul server. Dopo aver caricato un'immagine sul controller di gestione, è possibile anche spostare l'immagine caricata sul controller di gestione di un server differente. Quando si sposta l'immagine, l'immagine precedentemente caricata viene rimossa dal server corrente e caricata su un server selezionato.

- **Sposta supporti remoti**

  Questa azione sposta una risorsa del supporto precedentemente montato tra i server.

  Completare le seguenti operazioni per rendere disponibile una risorsa su un server:

  1. Selezionare una o più risorse.
  2. Fare clic su **Aggiungi** per spostare le risorse nell'elenco **Risorse selezionate**.
  3. Fare clic su **Monta** per montare le risorse che il server deve utilizzare. La sessione di controllo remoto definisce un dispositivo per la risorsa e associa il dispositivo a un punto di

montaggio del server correntemente selezionato. È possibile selezionare l'opzione di protezione dalla scrittura dei supporti montati.

Caricamento di un'immagine sul server

È inoltre possibile caricare un'immagine nello storage locale disponibile sul controller di gestione della scheda di base del server selezionato.

Informazioni su questa attività

L'immagine resta nel controller di gestione anche se la sessione di controllo remoto viene terminata o il server viene riavviato.

Nel controller di gestione è possibile archiviare circa 50 MB di dati.

È possibile caricare più immagini nel controller di gestione, a condizione che lo spazio totale utilizzato per tutte le immagini sia inferiore a 50 MB.

Ogni immagine che viene caricata nel controller di gestione viene montata automaticamente sul server. Dopo aver caricato un'immagine sul controller di gestione, è possibile anche spostare l'immagine caricata sul controller di gestione di un server differente. Quando si sposta l'immagine, l'immagine precedentemente caricata viene rimossa dal server corrente e caricata su un server selezionato.

Procedura

Per caricare un'immagine sul server, completare la seguente procedura.

Passo 1. Dalla finestra Controllo remoto, fare clic sull'icona **Supporti remoti** ().

Passo 2. Fare clic su **Monta supporti remoti**.

Passo 3. Fare clic su **Carica l'immagine su IMM**.

Importazione ed esportazione delle impostazioni utente

È possibile scegliere di importare o esportare le impostazioni utente per la sessione di controllo remoto corrente.

Informazioni su questa attività

Quando si esportano le impostazioni utente, tutte le impostazioni utente della sessione di controllo remoto corrente vengono memorizzate in un file delle proprietà nel sistema locale. È possibile copiare il file delle proprietà in un altro sistema e importare le impostazioni nell'applicazione di controllo remoto per utilizzarle.

Procedura

Per importare o esportare le impostazioni utente per la sessione di controllo remoto corrente, completare la seguente procedura.

Passo 1. Dalla finestra Controllo remoto, fare clic sull'icona **Preferenza** ().

Passo 2. Fare clic sulla scheda **Impostazioni utente**.

Passo 3. Fare clic su **Importa** per importare le impostazioni da un file esportato oppure fare clic su **Esporta** per salvare tutte le impostazioni utente correnti in un file delle proprietà nel sistema locale.

Impostazione delle preferenze di controllo remoto

È possibile modificare le impostazioni delle preferenze per la sessione di controllo remoto corrente.

Procedura

Completare le seguenti operazioni per modificare le preferenze di controllo remoto.

Passo 1. Per modificare le preferenze di controllo remoto, fare clic sull'icona **Preferenze** (). Tutte le modifiche saranno effettive immediatamente.

- **KVM**
  - **Percentuale della larghezza di banda video**. L'aumento della larghezza di banda migliora la qualità di visualizzazione della sessione di controllo remoto ma potrebbe incidere sulle prestazioni della sessione di controllo remoto.
  - **Percentuale di frame aggiornati**. L'aumento della percentuale di frame aggiornati incrementa l'intervallo di aggiornamento della sessione di controllo remoto ma potrebbe incidere sulle prestazioni della sessione di controllo remoto.
  - **Tipo di tastiera**. Selezionare il tipo di tastiera che si utilizza per la sessione di controllo remoto. Il tipo di tastiera selezionato deve corrispondere alle configurazioni della tastiera del sistema locale e dell'host remoto.

    Nota: Se si seleziona una tastiera internazionale ed è necessario immettere una combinazione di tasti che richiede l'utilizzo del tasto AltGr (Alternate Graphics), verificare che il sistema operativo della workstation usata per richiamare la sessione di controllo remoto sia dello stesso tipo di quello del server a cui si desidera accedere in remoto. Ad esempio, se sul server è in esecuzione Linux, assicurarsi di richiamare l'applicazione di controllo remoto da una workstation Linux.
  - **Adatta immagine a finestra**. Selezionare questa opzione per adattare l'immagine video ricevuta dal server alla dimensione dell'area delle sessioni video.
- **Protezione**
  - **Preferisci connessioni modalità utente singolo**. Specificare se le connessioni modalità utente singolo sono l'impostazione predefinita per il collegamento a un server. Quando viene stabilita una connessione in modalità utente singolo, solo un utente per volta può essere collegato a un server. Se questa casella non è selezionata, la funzione predefinita è il collegamento al server in modalità multiutente.
  - **Richiedi connessioni tunneling (sicure)**. Selezionare questa opzione per accedere a un server tramite il nodo di gestione. È possibile utilizzare questa opzione per accedere a un server da un client che non si trova nella stessa rete del server.

    Nota: L'applicazione di controllo remoto tenta sempre di collegarsi direttamente al server dal sistema locale dove il controllo remoto è stato avviato. Se la workstation client non può accedere direttamente al server, selezionando questa opzione, l'applicazione di controllo remoto accede al server tramite Lenovo XClarity Administrator.
- **Barra degli strumenti**

  Nota: Fare clic su **Ripristina valori predefiniti** per ripristinare tutte le impostazioni in questa pagina ai valori predefiniti
  - **Aggiungi la barra degli strumenti alla finestra**. Per impostazione predefinita, la barra degli strumenti è nascosta sopra la finestra della sessione di controllo remoto e viene visualizzata solo al passaggio del mouse. Se si seleziona questa opzione, la barra di strumenti viene aggiunta alla finestra e viene sempre visualizzata tra il pannello della miniatura e la finestra della sessione di controllo remoto.
  - **Mostra pulsanti tastiera**. Consente di specificare se visualizzare le icone dei pulsanti della tastiera (BlocMaiusc, BlocNum e BlocScorr) sulla barra degli strumenti.

- **Mostra controllo alimentazione**. Consente di specificare se visualizzare le opzioni di controllo dell'alimentazione sulla barra degli strumenti.
- **Mostra pulsanti con tasti permanenti**. Consente di specificare se visualizzare le icone dei pulsanti con tasti permanenti (Ctrl, Alt e Canc) sulla barra degli strumenti.
- **Nascondi puntatore mouse locale**. Consente di specificare se visualizzare il puntatore del mouse locale quando si posiziona il cursore nella sessione server attualmente visualizzata nell'area delle sessioni video.
- **Abilita modalità di acquisizione mouse**. Per impostazione predefinita, la modalità di acquisizione del mouse è disabilitata. Ciò significa che è possibile spostare liberamente il cursore all'interno e all'esterno dell'area delle sessioni video. Se si abilita la modalità di acquisizione mouse, è necessario premere il tasto Alt sinistro prima di poter spostare il cursore all'esterno dell'area delle sessioni video. Se la modalità di acquisizione mouse è abilitata, è possibile specificare se utilizzare i tasti Ctrl+Alt per uscire dalla modalità di acquisizione mouse. L'impostazione predefinita è l'uso del tasto Alt sinistro.
- **Specifica opacità sfondo barra degli strumenti**. La riduzione della percentuale di opacità consente di visualizzare un'area maggiore della sessione video attraverso lo sfondo della barra degli strumenti.

  Nota: Questa opzione è disponibile solo quando la barra degli strumenti non è stata aggiunta alla finestra.

- **Miniature**
  - **Mostra miniature**. Selezionare questa opzione per mostrare l'area miniature nella sessione di controllo remoto.
  - **Specifica intervallo di aggiornamento miniature**. Riducendo l'intervallo di aggiornamento delle miniature viene aumentata la frequenza di aggiornamento delle miniature dei server.
- **Generale**
  - **Modalità di debug**. Consente di specificare se impostare la modalità di debug per l'applicazione di controllo remoto. Le impostazioni determinano la granularità degli eventi registrati nei file di log. Per impostazione predefinita, vengono registrati solo gli eventi gravi. Per ulteriori informazioni sulle posizioni dei file di log, vedere Visualizzazione di log e tracce di controllo remoto.
  - **Eredita impostazioni aspetto sistema**. Questa impostazione modifica l'aspetto in modo che corrisponda alla combinazione di colori configurata per il server locale (basato su Windows). Per rendere effettive queste impostazioni, è necessario riavviare l'applicazione di controllo remoto.
  - C**rea icona sul desktop**. Questa impostazione crea un'icona sul desktop del sistema locale in modo da poter avviare l'applicazione di controllo remoto direttamente dal sistema. È necessario disporre dell'accesso al software di gestione del sistema.
  - **Sincronizza con il server di gestione**. Questa impostazione verifica che i dati del server visualizzati nell'applicazione di controllo remoto corrispondano ai dati del server visualizzati dal software di gestione.

Visualizzazione di log e tracce di controllo remoto

Quando si avvia una sessione di controllo remoto, vengono creati i file di log. I tipi di eventi registrati in questi file sono basati sulla modalità di debug, impostata dalla scheda **Generale** nella finestra di dialogo Preferenze. È possibile utilizzare questi file di log per risolvere i problemi.

Procedura

I file di log di controllo remoto vengono memorizzati nelle seguenti posizioni.

Sistema operativo	Directory dei log:
Windows 7 e 8	%USERPROFILE%\lenovo\remoteaccess Ad esempio: C:\Users\win_user\lenovo\remoteaccess

Per ulteriori informazioni sulla raccolta dei file di diagnostica e sull'invio dei file a Supporto Lenovo, vedere Utilizzo di assistenza e supporto nella documentazione online di Lenovo XClarity Administrator.

Gestione dell'accesso ai sistemi operativi sui server gestiti

È possibile gestire l'accesso ai sistemi operativi sui server gestiti.

Prima di iniziare

È necessario disporre dell'autorità **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** o **lxc-hw-admin** per gestire e distribuire i driver di dispositivo, nonché per eseguire azioni di alimentazione sui server gestiti dalle pagine "Aggiornamenti dei driver di Windows".

Informazioni su questa attività

Prima che Lenovo XClarity Administrator possa aggiornare i driver di dispositivo del sistema operativo su un sistema gestito, è necessario fornire le informazioni per accedere al sistema operativo host, come l'indirizzo IP e le credenziali memorizzate dell'amministratore per accedere al sistema operativo host. Per ulteriori informazioni sull'aggiornamento dei driver di dispositivo del sistema operativo, vedere Aggiornamento dei driver di dispositivo di Windows sui server gestiti.

XClarity Administrator utilizza le credenziali memorizzate per eseguire l'autenticazione con il sistema operativo host. Per ulteriori informazioni sulla creazione delle credenziali memorizzate in XClarity Administrator, vedere Gestione delle credenziali memorizzate.

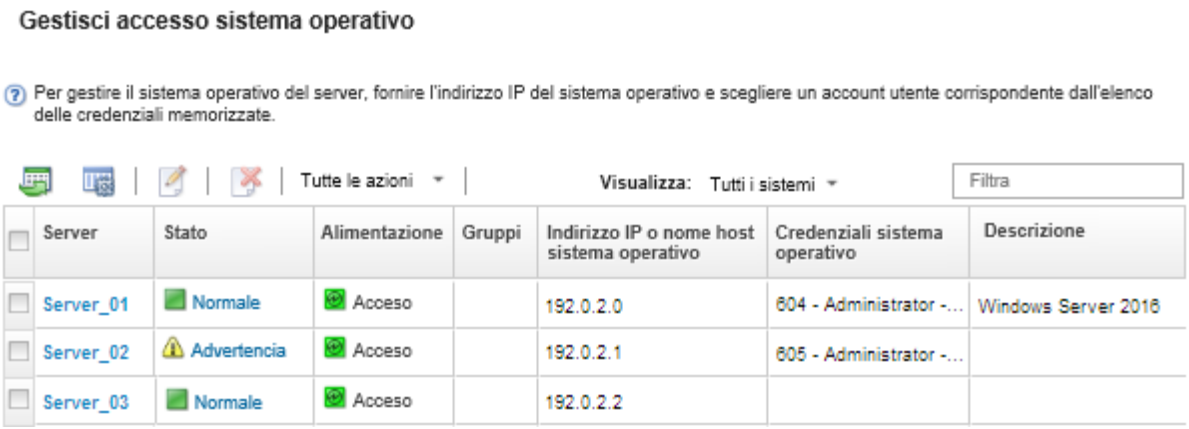
Suggerimento: XClarity Administrator non convalida automaticamente le informazioni specificate in questa pagina.

Procedura

Completare le seguenti operazioni per modificare le proprietà del sistema operativo.

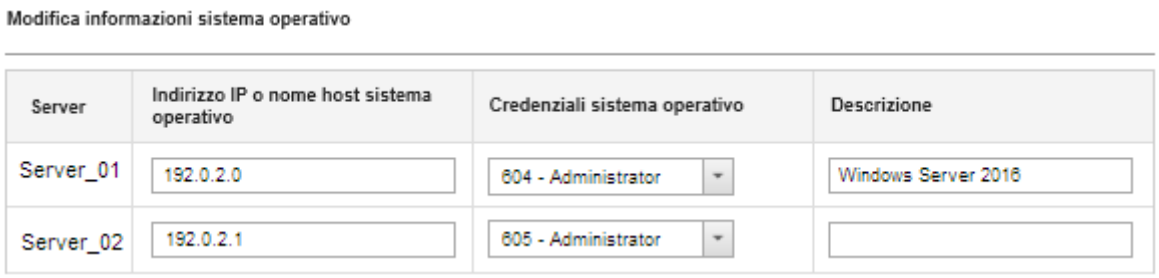
Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci accesso al sistema operativo** per visualizzare la pagina Gestisci accesso al sistema operativo.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. Inoltre, è possibile selezionare un tipo di sistema dall'elenco a discesa **Tutti i sistemi** e immettere testo (ad esempio un nome di sistema o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i server visualizzati.



Passo 2. Selezionare i server da aggiornare.

Passo 3. Fare clic sull'icona **Modifica informazioni sistema operativo** ( ) per visualizzare la finestra di dialogo Modifica informazioni sistema operativo.



Passo 4. Per ciascun server di destinazione, specificare le seguenti informazioni:
- Indirizzo IP o nome host del sistema operativo host
- (Facoltativo) Credenziali memorizzate per accedere al sistema operativo host
- (Facoltativo) Descrizione del sistema operativo host

Passo 5. Fare clic su **Salva**.

Al termine

È possibile eseguire le seguenti azioni per gestire l'accesso al sistema operativo.

- Cancellare le informazioni del sistema operativo (indirizzo IP, credenziali e descrizione), selezionando il server e facendo clic sull'icona **Rimuovi informazioni sistema operativo** ( ).
- Eseguire un test dell'autenticazione sui server Windows facendo clic su **Provisioning → Aggiornamenti dei driver di Windows: Applica**, selezionando il server di destinazione e quindi facendo clic su **Controlla autenticazione**.
- Visualizzare le informazioni sulla distribuzione per il sistema operativo su un server specifico passando il puntatore del mouse sul nome del server.

  Nota: Le informazioni sulla distribuzione sono disponibili solo per i sistemi operativi correttamente distribuiti dall'istanza di XClarity Administrator. Le informazioni sulla distribuzione non sono disponibili per le distribuzioni non riuscite e per le distribuzioni eseguite con altri mezzi, quale un'altra istanza di XClarity Administrator.

Visualizzazione delle chiavi Features on Demand

È possibile visualizzare un elenco delle chiavi Features on Demand attualmente installate sui server gestiti.

Informazioni su questa attività

Non è possibile acquistare, installare, o gestire la chiave Features on Demand dall'interfaccia Web di Lenovo XClarity Administrator. Per informazioni sull'acquisizione e l'installazione delle chiavi Features on Demand, vedere Features on Demand nella documentazione online di XClarity Administrator.

Procedura

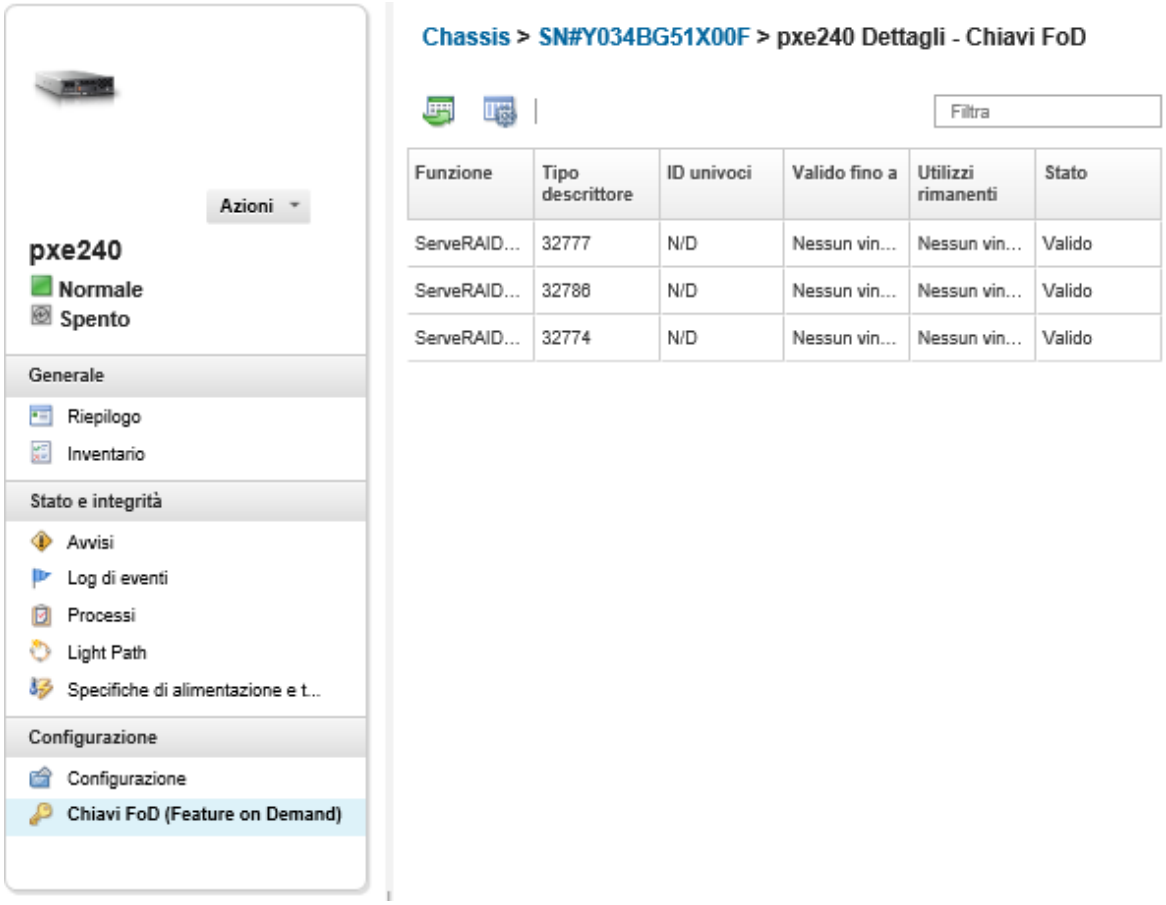
Completare le seguenti operazioni per visualizzare un elenco delle chiavi FoD installate in un server gestito specifico.

Passo 1. Dal menu XClarity Administrator, fare clic su **Hardware → Server**. Verrà visualizzata la pagina Server contenente una vista tabulare di tutti i server gestiti (rack/tower e nodi di elaborazione).

Passo 2. Fare clic sul nome del server nella colonna **Server**. Viene visualizzata la pagina di riepilogo dello stato del server, che mostra le proprietà del server e un elenco dei componenti installati nel server.

Passo 3. Fare clic su **Dettagli inventario** in Generale nel pannello di navigazione sinistro ed espandere la sezione dei singoli componenti hardware per visualizzare gli ID univoci FoD per tali componenti.

Passo 4. Fare clic su Chiavi **Features on Demand** in Configurazione nel pannello di navigazione sinistro per visualizzare informazioni su tutte le chiavi FoD installate sul server.



Gestione di alimentazione e temperatura

È possibile monitorare e gestire il consumo energetico e la temperatura dei server Converged, NeXtScale, System x e ThinkServer, nonché migliorare l'efficienza energetica mediante Lenovo XClarity Energy Manager.

Ulteriori informazioni:  Lenovo XClarity Energy Manager

Informazioni su questa attività

XClarity Administrator è un'interfaccia utente autonoma che è possibile utilizzare per monitorare e gestire il consumo energetico e la temperatura dei server supportati, tra cui:

- Monitoraggio del consumo energetico, stima della richiesta energetica e ridistribuzione dell'alimentazione ai server in base alle esigenze.
- Monitoraggio della temperatura e della capacità di raffreddamento dei server.
- Invio di notifiche al verificarsi di determinati eventi o in caso di superamento delle soglie.
- Limitazione della quantità di energia utilizzata da un dispositivo tramite criteri.
- Ottimizzazione dell'efficienza energetica attraverso il monitoraggio in tempo reale delle temperature in ingresso, identificazione dei server a basso consumo in base ai dati energetici fuori banda, misurazione degli intervalli di potenza per modelli di server diversi e valutazione dei modi in cui i server possono supportare nuovi carichi di lavoro in base alla disponibilità delle risorse.
- Riduzione del consumo energetico ai minimi livelli per prolungare i tempi di servizio durante situazioni di emergenza (ad esempio, in caso di interruzione dell'alimentazione del centro dati).

Per ulteriori informazioni sulle procedure di download, installazione e utilizzo di XClarity Administrator, vedere Sito Web di Lenovo XClarity Energy Manager.

Accensione e spegnimento di un server

È possibile accendere e spegnere un server da Lenovo XClarity Administrator.

Prima di iniziare

- Per Red Hat® Enterprise Linux (RHEL) v7 e versioni successive, riavviare il sistema operativo da una modalità grafica consente di sospendere il server per impostazione predefinita. Prima di poter eseguire le azioni **Riavvia normalmente** o **Riavvia immediatamente** da XClarity Administrator, è necessario configurare manualmente il sistema operativo per modificare il comportamento del pulsante di alimentazione su Spegni. Per istruzioni, vedere Guida di amministrazione e migrazione dei dati di Red Hat: modifica del comportamento in caso di pressione del pulsante di alimentazione in modalità di destinazione grafica.
- Per SLES Linux Enterprise Server (SLES), per spegnere il sistema operativo è necessario immettere la password radice nella sessione SLES. Per poter eseguire le azioni **Spegni normalmente** o **Spegni immediatamente** da XClarity Administrator, è necessario spegnere manualmente il server mediante l'interfaccia SLES locale e selezionare l'opzione **Remember authentication** (Ricorda autenticazione) quando si immette la password oppure controllare i criteri di sicurezza per verificare la possibilità di disabilitare l'autenticazione obbligatoria.
- Se abilitata, l'opzione di avvio WOL (Wake-on-LAN) può interferire con le operazioni di XClarity Administrator che spengono il server, inclusi gli aggiornamenti firmware se nella rete è presente un client Wake-on-LAN che genera comandi "Magic Packet per riattivazione".
- L'azione di alimentazione **Riavvia con la configurazione di sistema** riavvia il server, quindi apre BIOS/UEFI Setup Utility in una sessione di controllo remoto, anziché eseguire un normale avvio con sistema operativo.
- Le azioni di alimentazione **Spegni normalmente** e **Spegni immediatamente** variano a seconda delle configurazioni del sistema operativo installato sul dispositivo e funzionano solo se il sistema operativo è configurato per supportarle.
- È possibile riavviare il dispositivo con NMI (non-maskable interrupt) facendo clic su **Tutte le azioni → Servizio → Attiva NMI**.

Procedura

Per accendere o spegnere un server, attenersi alla procedura descritta di seguito.

Passo 1. Dal menu XClarity Administrator, fare clic su **Hardware → Server**. Viene visualizzata la pagina Server con una vista tabulare di tutti i server gestiti (server rack e nodi di elaborazione).

Passo 2. Selezionare il server.

Passo 3. Fare clic su **Tutte le azioni → Azioni di alimentazione**, quindi selezionare una delle seguenti azioni di alimentazione:
- **Accendi** consente di accendere il dispositivo.
- **Spegni normalmente** consente di arrestare il sistema operativo e di spegnere il dispositivo.
- **Spegni immediatamente** consente di spegnere il dispositivo.
- **Riavvia normalmente** consente di arrestare il sistema operativo e di riavviare il dispositivo.
- **Riavvia immediatamente** consente di riavviare il dispositivo
- **Riavvia con la configurazione di sistema** consente di riavviare il dispositivo con la configurazione BIOS/UEFI (F1). Questa operazione è supportata per i server ThinkServer che non prevedono limitazioni.
- **Riavvia controller di gestione** consente di riavviare il controller BMC.
- **Riavvia immediatamente e tenta l'avvio di rete PXE** consente di riavviare immediatamente il server e di avviarlo nella rete PXE (Preboot Execution Environment). Questa operazione è supportata per i server Lenovo Flex System, System x e ThinkSystem.

  Nota: Le impostazioni UEFI relative all'avvio PXE devono essere configurate sul server.

Riposizionamento virtuale di un server in uno chassis di Flex System

È possibile simulare la rimozione e il reinserimento di un server in uno chassis di Flex System riavviando il server mediante NMI (non-maskable interrupt).

Informazioni su questa attività

Durante il riposizionamento virtuale, tutte le connessioni di rete esistenti sul server andranno perse e lo stato di alimentazione del server verrà modificato. Prima di eseguire un riposizionamento virtuale, accertarsi di aver salvato tutti i dati utente.

Attenzione:

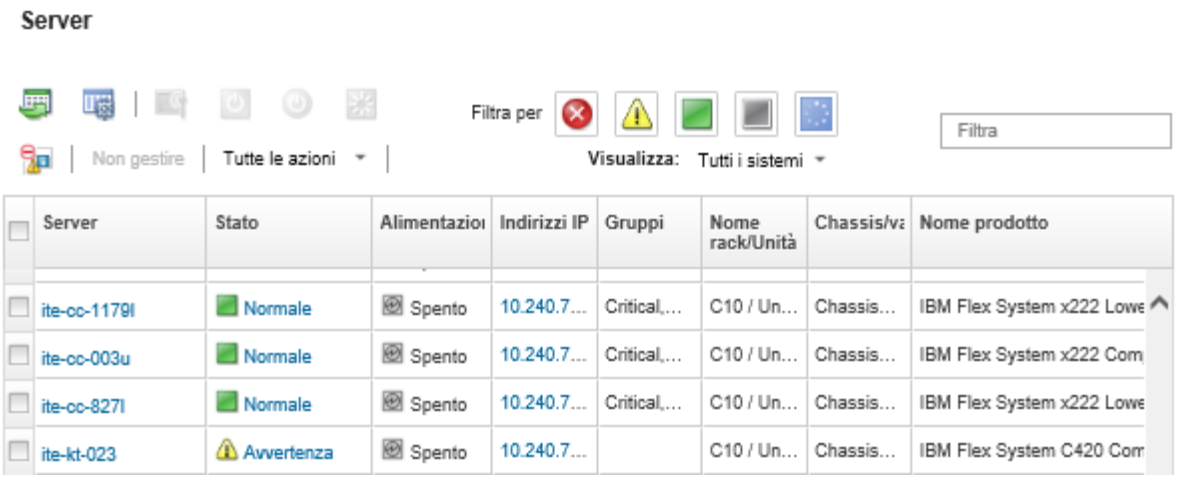
- Non eseguire un riposizionamento virtuale, se non richiesto da Supporto Lenovo.
- L'esecuzione di un riposizionamento virtuale potrebbe determinare la perdita di dati. Prima di riposizionare il server, eseguire le operazioni necessarie per proteggere i dati utenti.
- Anziché eseguire un riposizionamento virtuale, valutare la possibilità di spegnere il server. Per informazioni sulle azioni di alimentazione, vedere Accensione e spegnimento di un server.

Procedura

Completare le seguenti operazioni per riposizionare virtualmente un server in uno chassis di Flex System.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware → Server**. Verrà visualizzata la pagina Server contenente una vista tabulare di tutti i server gestiti.

È possibile ordinare le colonne della tabella per individuare più facilmente il server che si desidera riposizionare. Inoltre, è possibile selezionare un tipo di dispositivo dall'elenco a discesa **Tutti i dispositivi** e immettere del testo (come un nome o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i server visualizzati.



Passo 2. Selezionare il server nella tabella.

Passo 3. Fare clic su **Tutte le azioni → Servizio → Riposizionamento virtuale**.

Passo 4. Fare clic su **Riposizionamento virtuale**.

Avvio dell'interfaccia del controller di gestione per un server

È possibile avviare l'interfaccia Web del controller di gestione per un server specifico da Lenovo XClarity Administrator.

Prima di iniziare

Per accedere ai server ThinkSystem SR635/SR655 tramite XClarity Administrator, un utente deve disporre dei privilegi **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** o **lxc-os-admin** (vedere Gestione del server di autenticazione).

Quando si utilizza Single Sign-On, è possibile avviare l'interfaccia di gestione per un server gestito da XClarity Administrator, senza dover eseguire il login. L'opzione Single Sign-On è supportata per i server ThinkSystem e ThinkAgile (ad eccezione di SR635 e SR655). I server ThinkSystem SR645 e SR665 richiedono il firmware XCC 21A o versione successiva.

Per accedere direttamente al controller di gestione utilizzando gli account utente LDAP locali o esterni senza eseguire il login a XClarity Administrator, utilizzare l'URL `https://{XCC_IP_adderss}/#/login`.

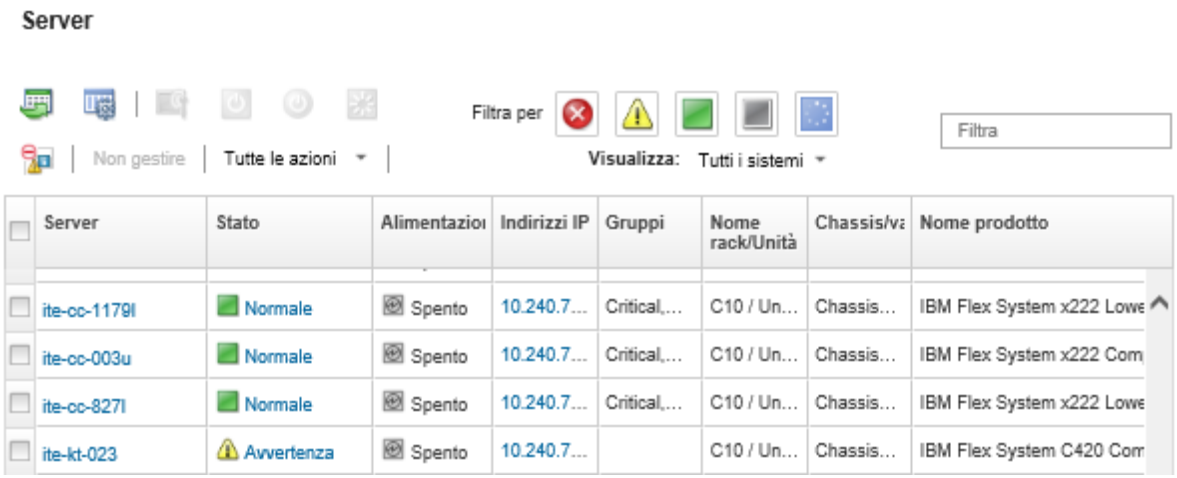
Procedura

Per avviare l'interfaccia del controller di gestione per un server, attenersi alla procedura descritta di seguito.

Nota: Non è supportato l'avvio di un'interfaccia del controller di gestione da Lenovo XClarity Administrator mediante il browser Web Safari.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Hardware → Server** per visualizzare la pagina Server.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. Inoltre, è possibile selezionare un tipo di sistema dall'elenco a discesa **Tutti i sistemi** e immettere del testo (come un nome o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i server visualizzati.



Passo 2. Fare clic sul collegamento per il server nella colonna **Server**. Verrà visualizzata la relativa pagina di riepilogo dello stato.

Passo 3. Fare clic su **Tutte le azioni → Avvia → Interfaccia Web di gestione**. Verrà avviata l'interfaccia Web del controller di gestione per il server.

Suggerimento: è inoltre possibile fare clic sull'indirizzo IP nella colonna **Indirizzi IP** per avviare l'interfaccia del controller di gestione.

Passo 4. Eseguire il login all'interfaccia del controller di gestione utilizzando le credenziali utente XClarity Administrator.

Al termine

Per ulteriori informazioni sull'utilizzo dell'interfaccia del controller di gestione per un server, vedere Documentazione online di Integrated Management Module II e Documentazione online di XClarity Controller.

Modifica delle proprietà di sistema per un server

È possibile modificare le proprietà di sistema per un server specifico.

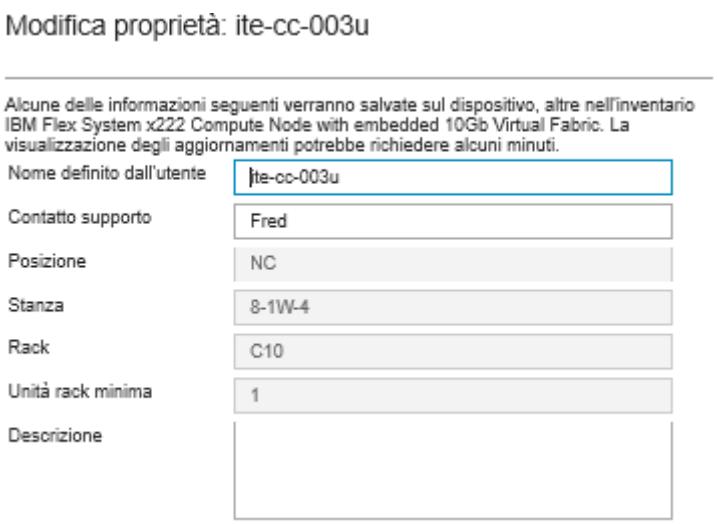
Procedura

Per modificare le proprietà di sistema, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Hardware → Server** per visualizzare la pagina Server.

Passo 2. Selezionare il server da aggiornare.

Passo 3. Fare clic su **Tutte le azioni → Inventario → Modifica proprietà** per visualizzare la finestra di dialogo Modifica.



Passo 4. Modificare le seguenti informazioni, in base alle esigenze.
- Nome definito dall'utente per il server
- Contatto supporto
- Descrizione

Nota: Posizione, ambiente, rack e proprietà dell'unità inferiore del rack vengono aggiornati da XClarity Administrator quando si aggiungono o rimuovono dispositivi da un rack nell'interfaccia Web (vedere Gestione dei rack).

Passo 5. Fare clic su **Salva**.

Nota: Quando vengono modificate queste proprietà, è possibile che si verifichi un breve ritardo nella visualizzazione delle modifiche nell'interfaccia Web di XClarity Administrator.

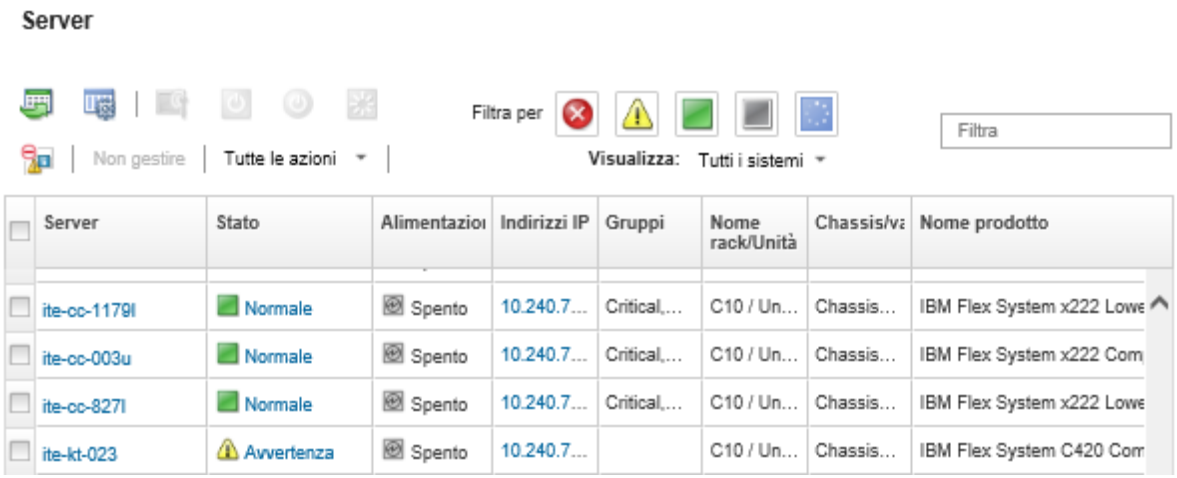
Risoluzione di credenziali memorizzate scadute o non valide per un server

Quando una credenziale memorizzata scade o non è più utilizzabili su un dispositivo, lo stato del dispositivo viene visualizzato come "Offline."

Procedura

Per risolvere le credenziali memorizzate scadute o non valide per un server.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware → Server**. Viene visualizzata la pagina Server con una vista tabulare di tutti i server gestiti (server rack e nodi di elaborazione).



Passo 2. Fare clic sull'intestazione di colonna di tabella **Alimentazione** per raggruppare tutti i server offline nella parte superiore della tabella.

Inoltre, è possibile selezionare un tipo di sistema dall'elenco a discesa Tutti i sistemi e immettere del testo (ad esempio un nome di sistema o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i server visualizzati.

Passo 3. Selezionare il server da risolvere.

Passo 4. Fare clic su **Tutte le azioni → Sicurezza → Modifica credenziali memorizzate**.

Passo 5. Modificare la password per la credenziale memorizzata o selezionare un'altra credenziale memorizzata da utilizzare per il dispositivo gestito.

Nota: Se è stato gestito più di un dispositivo utilizzando le stesse credenziali memorizzate ed è stata modificata la password per le credenziali memorizzate, la modifica della password interessa tutti i dispositivi che attualmente utilizzano le credenziali memorizzate.

Ripristino di un server guasto in seguito alla distribuzione di un pattern server

In caso di guasto di un server dopo la distribuzione di un pattern server, sarà possibile ripristinare il server annullando l'assegnazione del profilo dal server guasto e riassegnandolo a un server in standby.

Procedura

Completare le seguenti operazioni per ripristinare il server guasto che utilizza l'autenticazione gestita di Lenovo XClarity Administrator.

Passo 1. Identificare il server guasto.

Passo 2. Annullare l'assegnazione del profilo dal server guasto (vedere Disattivazione di un profilo del server).

Attenzione: Il server guasto deve essere spento per poter disattivare gli indirizzi virtuali assegnati *prima* di riassegnare il profilo. Quando si annulla l'assegnazione del profilo del server, selezionare **Spegni server** nella finestra di dialogo Rimuovi profilo server per spegnere il server guasto (vedere Accensione e spegnimento di un server).

Passo 3. Assegnare il profilo del server a un server in standby (vedere Attivazione di un profilo del server).

Passo 4. Attivare il profilo accendendo il server in standby se è spento oppure riavviandolo se è acceso (vedere Accensione e spegnimento di un server).

Passo 5. Eseguire la migrazione delle impostazioni VLAN negli switch associati al server in standby.

Passo 6. Assicurarsi che il server guasto sia spento.

Passo 7. Sostituire o ripristinare il server guasto. In caso di ripristino, effettuare le seguenti operazioni per accertarsi che siano state ripristinate le impostazioni predefinite per il server

a. Per ripristinare le impostazioni predefinite del controller BMC, utilizzare l'interfaccia Web di gestione del server. Per ulteriori informazioni sul ripristino di BMC, vedere Ripristino della gestione di server ThinkSystem, Converged, NeXtScale o System x M5 oppure M6 in seguito a un errore del server di gestione mediante la reimpostazione del controller di gestione.

b. Cancellare le informazioni UEFI (Unified Extensible Firmware Interface), inclusi eventuali indirizzi virtuali dell'adattatore I/O, mediante i menu UEFI. Per informazioni, vedere la documentazione UEFI.

Ripristino delle impostazioni di avvio in seguito alla distribuzione di pattern server

Se uno o più server non si avviano in seguito alla distribuzione di un nuovo pattern server, il problema potrebbe essere riconducibile al fatto che le impostazioni di avvio sono state sovrascritte dalle impostazioni di avvio predefinite nel pattern server. Per i sistemi operativi installati in modalità UEFI, il ripristino delle impostazioni predefinite potrebbe richiedere ulteriori passaggi per ripristinare la configurazione di avvio.

Procedura

Per consentire il ripristino delle impostazioni di avvio originali per ogni server coinvolto, attenersi alla seguente procedura di ripristino manuale.

- Per un server in cui è installato Red Hat Enterprise Linux:
  1. Se si accede al server in remoto, creare una sessione di controllo remoto al server (vedere Utilizzo del controllo remoto per gestire i server Converged, Flex System, NeXtScale e System x).
  2. Riavviare il server facendo clic su **Strumenti → Alimentazione → Attivato**. Se la schermata iniziale UEFI per il server è visualizzata nella sessione di controllo remoto, premere F1 per visualizzare Setup Utility.
  3. Selezionare **Boot Manager**.
  4. Selezionare **Add Boot Option**.
  5. Selezionare **UEFI Full Path Option**.
  6. Dall'elenco visualizzato selezionare una voce che includa `SAS`.
  7. Selezionare **EFI**.
  8. Selezionare **redhat**.
  9. Selezionare **grub.efi**.
  10. Selezionare il campo **Input the Description**.
  11. Digitare `Red Hat Enterprise Linux`.
  12. Selezionare **Commit Changes**.
  13. Rendere `Red Hat Enterprise Linux` la prima opzione in Ordine di avvio e rimuovere tutte le altre opzioni.
  14. Premere il tasto ESC, quindi selezionare **Save changes then exit this menu**.
  15. Premere il tasto ESC, quindi selezionare **Exit the Configuration Utility and Reboot**. Il nodo di elaborazione verrà riavviato.
- Per un server in cui è installato Microsoft Windows Server 2008:
  1. Accendere il server e, quando richiesto, premere F1 per accedere alla configurazione.
  2. Selezionare **Boot Manager**.

3. Selezionare **Boot from File**.
4. Selezionare la partizione di sistema GPT (GUID Partition Tables) in cui è stato installato Microsoft Windows Server 2008.
5. Selezionare **EFI**.
6. Selezionare **Microsoft**.
7. Selezionare **Boot**.
8. Selezionare **bootmgfw.EFI**.

Nota: Per ulteriori informazioni, vedere Suggerimento di tipo RETAIN 5079636.

Ripristino della gestione del server tower o rack dopo un errore del server di gestione

Se un server rack o tower è gestito da Lenovo XClarity Administrator e si verificano errori in XClarity Administrator, è possibile ripristinare le funzioni di gestione finché XClarity Administrator non verrà ripristinato o sostituito.

Informazioni su questa attività

Per ripristinare la gestione per un server Flex System, vedere Ripristino della gestione con un modulo CMM dopo un errore del server di gestione.

Ripristino della gestione di server tower o rack in seguito a un errore del server di gestione mediante Forza gestione

È possibile ripristinare la gestione server gestendo nuovamente il server mediante l'opzione Forza gestione

Procedura

Se l'istanza di sostituzione di Lenovo XClarity Administrator utilizza lo stesso indirizzo IP dell'istanza di XClarity Administrator con errori, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password `RECOVERY_ID` e l'opzione **Forza gestione** (vedere Gestione dei server).

Ripristino di un server System x o NeXtScale M4 la cui gestione non è stata annullata correttamente mediante il controller di gestione

È possibile ripristinare la gestione di un server System x o NeXtScale M4 mediante il controller di gestione della scheda di base.

Procedura

Completare le seguenti operazioni per ripristinare la gestione di un server che utilizza l'autenticazione gestita di Lenovo XClarity Administrator.

Passo 1. Accedere all'interfaccia Web del controller di gestione utilizzando l'account utente e la password creati prima della gestione del server da parte di XClarity Administrator

Passo 2. Cancellare le impostazioni trap SNMP.

a. Fare clic su **Gestione IMM → Rete**.
b. Fare clic sulla scheda **SNMP**.
c. Fare clic sulla scheda **Comunità**.

d. Individuare ad esempio la voce della comunità per l'istanza precedente di XClarity Administrator.
   - **Indirizzo IP LXCA:** 10.240.198.84
   - **Host LXCA:** LXCA_maqCBIt86d
   - **Comunità 2:**
   - **Nome della comunità:** LXCA_maqCBIt86d
   - **Tipo di accesso:** Trap
   - **Consenti a host specifici di ricevere trap in questa comunità:** 10.240.198.84

e. Rimuovere il valore nei campi per la voce della comunità.

f. Fare clic su **Applica**.

Passo 3. Cancellare gli account utente.

a. Fare clic su **Gestione IMM → Utenti**.

b. Fare clic sulla scheda **Account utente**.

c. Eliminare tutti gli account utente XClarity Administrator, inclusi gli account utente con i seguenti prefissi:
   - DISABLE_*
   - LXCA_*
   - OBSOLETE_*
   - SNMPCFGUSER

Al termine

Una volta ripristinato o sostituito XClarity Administrator, il server System x o NeXtScale potrà essere nuovamente gestito (vedere Gestione dei server). Verranno mantenute tutte le informazioni sul server (tra cui impostazioni di rete, criteri server e criteri di conformità del firmware).

Ripristino della gestione di server ThinkSystem, Converged, NeXtScale o System x M5 oppure M6 in seguito a un errore del server di gestione mediante la reimpostazione del controller di gestione

È possibile ripristinare la gestione di un server ThinkSystem, Converged, NeXtScale o System x M5 oppure M6 ripristinando i valori predefiniti del controller di gestione della scheda di base nel server.

Procedura

Completare le seguenti operazioni per recuperare la gestione di un server che utilizza l'autenticazione gestita di Lenovo XClarity Administrator.

Passo 1. Se Incapsulamento è abilitato nel dispositivo, connettersi al controller di gestione di destinazione da un sistema configurato per l'utilizzo dell'indirizzo IP dell'appliance virtuale XClarity Administrator con errori.

Passo 2. Ripristinare i valori predefiniti del controller di gestione.

a. Accedere all'interfaccia Web del controller di gestione per il server utilizzando l'account utente e la password di ripristino creati prima della gestione del server da parte di XClarity Administrator.

b. Fare clic sulla **scheda Gestione IMM**.

c. Fare clic su **Ripristina valori predefiniti originali IMM**.

d. Per confermare l'azione di ripristino, fare clic su **OK**.

Importante: una volta completata la configurazione di BMC, BMC verrà riavviato. Se questo è un server locale, la connessione TCP/IP viene interrotta e sarà necessario riconfigurare l'interfaccia di rete per ripristinare la connettività.

Passo 3. Accedere nuovamente all'interfaccia Web del controller di gestione per il server.

- Il controller BMC viene inizialmente configurato con l'intento di ottenere un indirizzo IP da un server DHCP. In caso di esito negativo, utilizzerà l'indirizzo IPv4 statico `192.168.70.125`.
- IMMBMC viene inizialmente impostato con il nome utente `USERID` e la password `PASSWORD` (con uno zero). Questo account utente predefinito ha accesso da supervisore. Per una maggiore sicurezza, modificare questo nome utente e la password durante la configurazione iniziale.

Passo 4. Riconfigurare l'interfaccia di rete per ripristinare la connettività. Per ulteriori informazioni, consultare la sezione Documentazione online di Integrated Management Module II.

Al termine

Una volta ripristinato o sostituito XClarity Administrator, il server potrà essere nuovamente gestito (vedere Gestione dei server). Verranno mantenute tutte le informazioni sul server (tra cui impostazioni di rete, criteri server e criteri di conformità del firmware).

Se il server è stato configurato mediante Pattern di configurazione, è possibile disattivare e quindi riattivare il profilo del server assegnato al server per applicare la configurazione (vedere Utilizzo di profili del server).

Ripristino della gestione di server ThinkSystem, Converged, NeXtScale o System x M5 oppure M6 in seguito a un errore del server di gestione mediante cimcli

È possibile ripristinare la gestione di un server ThinkSystem, Converged, NeXtScale o System x M5 oppure M6 mediante l'utility `cimcli` per cancellare le sottoscrizioni CIM.

Prima di iniziare

È necessario installare OpenPegasus con la utility cimcli in un sistema con accesso di rete al server di destinazione. Per informazioni sul download, sulla configurazione e sulla compilazione di OpenPegasus, vedere Sito Web degli RPM delle versioni di OpenPegasus per Linux.

Nota: Per Red Hat Enterprise Linux (RHEL) Server 7 e versioni successive, la distribuzione di Red Hat include RPM OpenPegasus sorgenti e binari. Il pacchetto `top-pegasus-test.x86_64` include la utility cimcli.

Informazioni su questa attività

Una volta ripristinato il server, sarà possibile gestirlo nuovamente. Verranno mantenute tutte le informazioni sul server (tra cui impostazioni di rete, criteri server e criteri di conformità del firmware).

Procedura

Completare la seguente procedura da un server che utilizza l'autenticazione gestita di Lenovo XClarity Administrator e su cui è installato OpenPegasus per ripristinare la gestione del server.

Passo 1. Se Incapsulamento è abilitato sul dispositivo:

a. Connettersi al server di destinazione da un sistema configurato per l'utilizzo dell'indirizzo IP dell'appliance virtuale XClarity Administrator con errori.

b. Disabilitare Incapsulamento aprendo una sessione SSH nel dispositivo ed eseguendo il seguente comando:

```
encaps lite off
```

Passo 2. Per determinare le istanze CIM per CIM_ListenerDestinationCIMXML, CIM_Indicationfilter e CIM_IndicationSubscription, eseguire i comandi riportati di seguito.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

dove <*IP_address*>, <*user_ID*> e <*password*> sono l'indirizzo IP, l'ID utente e la password per il controller di gestione. Ad esempio:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Passo 3. Per eliminare individualmente ogni istanza CIM per CIM_ListenerDestinationCIMXML, CIM_Indicationfilter e CIM_IndicationSubscription, eseguire il comando riportato di seguito.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

dove <*IP_address*>, <*user_ID*> e <*password*> sono l'indirizzo IP, l'ID utente e la password per il controller di gestione e <*cim_instance*> sono le informazioni restituite per ogni istanza CIM nel passaggio precedente, racchiuse tra virgolette singole. Ad esempio:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
```

```
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Al termine

Una volta ripristinato o sostituito Lenovo XClarity Administrator, il server System x o NeXtScale potrà essere nuovamente gestito (vedere Gestione dei server). Verranno mantenute tutte le informazioni sul server (tra cui impostazioni di rete, criteri server e criteri di conformità del firmware).

Ripristino della gestione di server ThinkServer in seguito a un errore del server di gestione mediante l'interfaccia del controller di gestione

È possibile ripristinare la gestione di un server ThinkServer dall'interfaccia del controller di gestione.

Procedura

Per ripristinare la gestione server, attenersi alla procedura descritta di seguito.

Passo 1. Eseguire il login come amministratore all'interfaccia Web del controller di gestione per il server (vedere Avvio dell'interfaccia del controller di gestione per un server).

Passo 2. Rimuovere gli account IPMI creati da Lenovo XClarity Administrator selezionando Utenti nel menu principale e quindi rimuovendo tutti gli account utente con il prefisso "LXCA_".

In alternativa, è possibile rinominare il nome utente dell'account e rimuovere il prefisso "LXCA_".

Passo 3. Per rimuovere le destinazioni trap SNMP, selezionare **Gestione PEF** nel menu principale, fare clic sulla scheda **Destinazione LAN** e rimuovere la voce che punta all'indirizzo IP dell'istanza di XClarity Administrator.

Passo 4. Per verificare la validità delle impostazioni NTP, selezionare **Impostazioni NTP** nel menu principale, quindi configurare manualmente la data e l'ora oppure fornire un indirizzo del server NTP valido.

Annullamento della gestione di un server rack o tower

È possibile rimuovere la gestione di un server rack o tower mediante Lenovo XClarity Administrator. Questo processo è detto *annullamento della gestione.*

Prima di iniziare

È possibile abilitare XClarity Administrator per annullare automaticamente la gestione dei dispositivi che restano offline per un periodo di tempo specifico. Questa opzione è disabilitata per impostazione predefinita. Per abilitare l'annullamento della gestione automatica dei dispositivi offline, fare clic su **Hardware → Rileva e gestisci nuovi dispositivi** dal menu di XClarity Administrator, quindi fare clic su **Modifica** accanto a **Annulla gestione dispositivi offline è Disabilitato**. Quindi, selezionare **Abilita annullamento gestione dispositivi offline** e impostare l'intervallo di tempo. Per impostazione predefinita, i dispositivi non vengono gestiti dopo essere rimasti offline per 24 ore.

Prima di annullare la gestione di un server rack o tower, accertarsi che nel server non siano in esecuzione processi attivi.

Se si desidera rimuovere il pattern server ed eventuali indirizzi virtuali nel server rack o tower, disattivare il profilo prima di annullare la gestione del server (vedere Disattivazione di un profilo del server).

Se la funzione Call Home è abilitata in XClarity Administrator, Call Home è disabilitata in tutti i server e gli chassis gestiti, al fine di evitare la creazione di record dei problemi duplicati. Se non si intende più utilizzare XClarity Administrator per gestire i dispositivi, sarà possibile riabilitare Call Home in tutti i dispositivi gestiti da XClarity Administrator anziché riabilitare Call Home per ogni singolo dispositivo in un secondo momento (vedere Riabilitazione di call home su tutti i dispositivi gestiti nella documentazione online di XClarity Administrator).

Informazioni su questa attività

Quando si annulla la gestione di un server rack o tower, Lenovo XClarity Administrator esegue le seguenti azioni:

- Cancella la configurazione utilizzata per la gestione utenti centralizzata.
- Rimuove il certificato di sicurezza del controller di gestione della scheda di base dall'archivio attendibile di XClarity Administrator.
- Se l'opzione Incapsulamento è abilitata sul dispositivo, configura le regole del firewall dei dispositivi con le impostazioni usate prima della gestione del dispositivo.
- Rimuove le sottoscrizioni CIM dalla configurazione di XClarity Administrator in modo che XClarity Administrator non riceva più gli eventi dal server rack o tower.
- Disabilita Call Home nel server rack o tower se Call Home è attualmente abilitato in XClarity Administrator.
- Rimuove gli eventi inviati dal server rack o tower. È possibile conservare questi eventi inoltrando gli eventi a un repository esterno, ad esempio un syslog (vedere Inoltro di eventi).

Se si annulla la gestione di un server rack o tower, XClarity Administrator mantiene determinate informazioni sul server. Queste informazioni verranno riapplicate quando lo stesso server rack o tower verrà nuovamente gestito.

Importante: Se si annulla la gestione di un server ThinkServer e quindi lo si gestisce in un'altra istanza di XClarity Administrator, le informazioni sul server andranno perse.

Suggerimento: tutti i dispositivi dimostrativi aggiunti facoltativamente durante la configurazione iniziale sono nodi di uno chassis. Per annullare la gestione dei dispositivi dimostrativi, annullare la gestione dello chassis mediante l'opzione **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.

Procedura

Per annullare la gestione di un server rack o tower, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Hardware → Server** per visualizzare la pagina Server.

Passo 2. Selezionare uno o più server rack o tower di cui annullare la gestione.

Passo 3. Fare clic su **Non gestire**. Viene visualizzata la finestra di dialogo Non gestire.

Passo 4. **Facoltativo:** selezionare **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.

Importante: quando si annulla la gestione di hardware dimostrativo, verificare di aver selezionato questa opzione.

Passo 5. Fare clic su **Non gestire**.La finestra di dialogo Non gestire mostra l'avanzamento di ogni operazione nel processo di annullamento della gestione.

Passo 6. Al termine del processo di annullamento della gestione, fare clic su **OK**.

Ripristino di un server rack o tower la cui gestione non è stata annullata correttamente

Se la gestione di un server Converged, NeXtScale, System x o ThinkServer non è stata annullata correttamente, è necessario ripristinare il server per poterlo gestire nuovamente.

Ripristino di un server rack o tower la cui gestione non è stata annullata correttamente mediante Forza gestione

È possibile ripristinare la gestione server gestendo nuovamente il server mediante l'opzione Forza gestione

Procedura

Se l'istanza di sostituzione di Lenovo XClarity Administrator utilizza lo stesso indirizzo IP dell'istanza di XClarity Administrator con errori, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password `RECOVERY_ID` e l'opzione **Forza gestione** (vedere Gestione dei server).

Ripristino di un server System x o NeXtScale M4 la cui gestione non è stata annullata correttamente mediante il controller di gestione

È possibile ripristinare la gestione di un server System x o NeXtScale M4 mediante il controller di gestione.

Procedura

Per ripristinare la gestione server, attenersi alla procedura descritta di seguito.

Passo 1. Accedere all'interfaccia Web del controller di gestione utilizzando l'account utente e la password creati prima della gestione del server da parte di XClarity Administrator

Passo 2. Cancellare le impostazioni trap SNMP.

a. Fare clic su **Gestione IMM → Rete**.

b. Fare clic sulla scheda **SNMP**.

c. Fare clic sulla scheda **Comunità**.

d. Individuare ad esempio la voce della comunità per l'istanza precedente di XClarity Administrator.
- **Indirizzo IP LXCA:** 10.240.198.84
- **Host LXCA:** LXCA_maqCBlt86d
- **Comunità 2:**
- **Nome della comunità:** LXCA_maqCBlt86d
- **Tipo di accesso:** Trap
- **Consenti a host specifici di ricevere trap in questa comunità:** 10.240.198.84

e. Rimuovere il valore nei campi per la voce della comunità.

f. Fare clic su **Applica**.

Passo 3. Cancellare gli account utente.

a. Fare clic su **Gestione IMM → Utenti**.

b. Fare clic sulla scheda **Account utente**.

c. Eliminare tutti gli account utente XClarity Administrator, inclusi gli account utente con i seguenti prefissi:
- DISABLE_*
- LXCA_*
- OBSOLETE_*
- SNMPCFGUSER

Passo 4. Gestire il server mediante Lenovo XClarity Administrator.

a. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci.

b. Selezionare **Immissione manuale**.

c. Fare clic su **Singolo sistema**, immettere l'indirizzo IP del server che si desidera gestire e scegliere **OK**.

d. Specificare l'ID utente e la password per l'autenticazione con il server.

e. Fare clic su **Gestisci**.

Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Monitorare l'avanzamento per garantire il completamento del processo.

f. Al termine del processo, fare clic su **OK**.

Ripristino di un server ThinkSystem, Converged, NeXtScale o System x M5 oppure M6 la cui gestione non è stata annullata correttamente, reimpostando i valori predefiniti del controller di gestione

È possibile ripristinare la gestione di un server ThinkSystem, Converged, NeXtScale o System x M5 oppure M6, reimpostando i valori predefiniti del controller di gestione della scheda di base nel server.

Procedura

Per ripristinare la gestione server, attenersi alla procedura descritta di seguito.

Passo 1. Se Incapsulamento è abilitato nel dispositivo, connettersi al controller di gestione di destinazione da un sistema configurato per l'utilizzo dell'indirizzo IP dell'appliance virtuale XClarity Administrator con errori.

Passo 2. Ripristinare i valori predefiniti del controller di gestione.

a. Accedere all'interfaccia Web del controller di gestione per il server utilizzando l'account utente e la password di ripristino creati prima della gestione del server da parte di XClarity Administrator.

b. Fare clic sulla **scheda Gestione IMM**.

c. Fare clic su **Ripristina valori predefiniti originali IMM**.

d. Per confermare l'azione di ripristino, fare clic su **OK**.

Importante: una volta completata la configurazione di BMC, BMC verrà riavviato. Se questo è un server locale, la connessione TCP/IP viene interrotta e sarà necessario riconfigurare l'interfaccia di rete per ripristinare la connettività.

Passo 3. Accedere nuovamente all'interfaccia Web del controller di gestione per il server.

- Il controller BMC viene inizialmente configurato con l'intento di ottenere un indirizzo IP da un server DHCP. In caso di esito negativo, utilizzerà l'indirizzo IPv4 statico `192.168.70.125`.
- IMMBMC viene inizialmente impostato con il nome utente `USERID` e la password `PASSWORD` (con uno zero). Questo account utente predefinito ha accesso da supervisore. Per una maggiore sicurezza, modificare questo nome utente e la password durante la configurazione iniziale.

Passo 4. Riconfigurare l'interfaccia di rete per ripristinare la connettività. Per ulteriori informazioni, consultare la sezione Documentazione online di Integrated Management Module II.

Passo 5. Gestire il server mediante Lenovo XClarity Administrator.

a. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci.

b. Selezionare **Immissione manuale**.

c. Fare clic su **Singolo sistema**, immettere l'indirizzo IP del server che si desidera gestire e scegliere **OK**.

d. Specificare l'ID utente e la password per l'autenticazione con il server.

e. Fare clic su **Gestisci**.

   Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Monitorare l'avanzamento per garantire il completamento del processo.

f. Al termine del processo, fare clic su **OK**.

Passo 6. Se il server è stato configurato mediante Pattern di configurazione, riattivare il profilo assegnato al server.

a. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Profili server**. Verrà visualizzata la pagina Pattern di configurazione: Profili server.

b. Selezionare il profilo del server e fare clic sull'icona **Disattiva profilo server** ().

c. Fare clic su **Spegni ITE** per spegnere il server. Alla riaccensione, verranno ripristinati i valori predefiniti integrati delle assegnazioni degli indirizzi virtuali.

d. Fare clic su **Disattiva**. Lo stato del profilo passa a "Inattivo" nella colonna Stato profilo. Nota: i server mantengono le informazioni identificative (ad esempio, nome host, indirizzo IP, indirizzo MAC virtuale) quando un profilo è disattivato.

e. Selezionare nuovamente il profilo del server e fare clic sull'icona **Attiva profilo server** ().

f. Fare clic su **Attiva** per attivare i profili nel server. Lo stato del profilo passa ad "Attivo" nella colonna Stato profilo.

Passo 7. Se al server sono stati assegnati criteri di conformità, riassegnarli.

a. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Applica/Attiva**. Verrà visualizzata la pagina Aggiornamenti firmware: Applica/Attiva con un elenco dei dispositivi gestiti.

b. Selezionare i criteri appropriati per il server dal menu a discesa nella colonna **Criteri assegnati**.

Ripristino di un server ThinkSystem, Converged, NeXtScale o System x M5 oppure M6 la cui gestione non è stata annullata correttamente mediante cimcli

È possibile ripristinare la gestione di un server ThinkSystem, Converged, NeXtScale o System x mediante l'utility `cimcli` per cancellare le sottoscrizioni CIM.

Prima di iniziare

È necessario installare OpenPegasus con la utility cimcli in un sistema con accesso di rete al server di destinazione. Per informazioni sul download, sulla configurazione e sulla compilazione di OpenPegasus, vedere Sito Web degli RPM delle versioni di OpenPegasus per Linux.

Nota: Per Red Hat Enterprise Linux (RHEL) Server 7 e versioni successive, la distribuzione di Red Hat include RPM OpenPegasus sorgenti e binari. Il pacchetto `top-pegasus-test.x86_64` include la utility cimcli.

Informazioni su questa attività

Una volta ripristinato il server, sarà possibile gestirlo nuovamente. Verranno mantenute tutte le informazioni sul server (tra cui impostazioni di rete, criteri server e criteri di conformità del firmware).

Procedura

Completare la seguente procedura da un server che utilizza l'autenticazione gestita di Lenovo XClarity Administrator e su cui è installato OpenPegasus per ripristinare la gestione del server.

Passo 1. Se Incapsulamento è abilitato sul dispositivo:

a. Connettersi al server di destinazione da un sistema configurato per l'utilizzo dell'indirizzo IP dell'appliance virtuale XClarity Administrator con errori.

b. Disabilitare Incapsulamento aprendo una sessione SSH nel dispositivo ed eseguendo il seguente comando:
```
encaps lite off
```

Passo 2. Per determinare le istanze CIM per CIM_ListenerDestinationCIMXML, CIM_Indicationfilter e CIM_IndicationSubscription, eseguire i comandi riportati di seguito.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

dove <*IP_address*>, <*user_ID*> e <*password*> sono l'indirizzo IP, l'ID utente e la password per il controller di gestione. Ad esempio:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Passo 3. Per eliminare individualmente ogni istanza CIM per CIM_ListenerDestinationCIMXML, CIM_Indicationfilter e CIM_IndicationSubscription, eseguire il comando riportato di seguito.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

dove <*IP_address*>, <*user_ID*> e <*password*> sono l'indirizzo IP, l'ID utente e la password per il controller di gestione e <*cim_instance*> sono le informazioni restituite per ogni istanza CIM nel passaggio precedente, racchiuse tra virgolette singole. Ad esempio:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
```

```
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Passo 4. Gestire il server mediante Lenovo XClarity Administrator.

a. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci.

b. Selezionare **Immissione manuale**.

c. Fare clic su **Singolo sistema**, immettere l'indirizzo IP del server che si desidera gestire e scegliere **OK**.

d. Specificare l'ID utente e la password per l'autenticazione con il server.

e. Fare clic su **Gestisci**.

Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Monitorare l'avanzamento per garantire il completamento del processo.

f. Al termine del processo, fare clic su **OK**.

Ripristino della gestione di un server ThinkServer la cui gestione non è stata annullata correttamente mediante l'interfaccia del controller di gestione

È possibile ripristinare la gestione di un server ThinkServer mediante l'interfaccia Web del controller di gestione.

Procedura

Per ripristinare la gestione server, attenersi alla procedura descritta di seguito.

Passo 1. Eseguire il login come amministratore all'interfaccia Web del controller di gestione per il server (vedere Avvio dell'interfaccia del controller di gestione per un server).

Passo 2. Rimuovere gli account IPMI creati da Lenovo XClarity Administrator selezionando Utenti nel menu principale e quindi rimuovendo tutti gli account utente con il prefisso "LXCA_".

In alternativa, è possibile rinominare il nome utente dell'account e rimuovere il prefisso "LXCA_".

Passo 3. Per rimuovere le destinazioni trap SNMP, selezionare **Gestione PEF** nel menu principale, fare clic sulla scheda **Destinazione LAN** e rimuovere la voce che punta all'indirizzo IP dell'istanza di XClarity Administrator.

Passo 4. Per verificare la validità delle impostazioni NTP, selezionare **Impostazioni NTP** nel menu principale, quindi configurare manualmente la data e l'ora oppure fornire un indirizzo del server NTP valido.

Capitolo 9. Gestione di dispositivi di storage

Lenovo XClarity Administrator consente di gestire diversi tipi di dispositivi di storage, tra cui Lenovo Storage, i sistemi di storage Flex System e le librerie a nastro.

Ulteriori informazioni:  XClarity Administrator: rilevamento

Prima di iniziare

Attenzione: Esaminare le Considerazioni sulla gestione dello storage prima di gestire un dispositivo di storage.

Nota: I dispositivi di storage Flex System vengono rilevati e gestiti automaticamente quando si gestisce lo chassis che li contiene. Non è possibile rilevare e gestire dispositivi di storage Flex System indipendenti dallo chassis.

Alcune porte devono essere disponibili per la comunicazione con i dispositivi. Accertarsi che tutte le porte necessarie siano disponibili prima di gestire i dispositivi di storage. Per informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.

Accertarsi che sia installato il firmware minimo richiesto in ciascun dispositivo di storage che si desidera gestire mediante XClarity Administrator. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.

Importante: Prima di rilevare e gestire i dispositivi di storage rack, verificare che i seguenti requisiti siano stati soddisfatti (diverso da ThinkSystem serie DE). Per ulteriori informazioni, vedere Impossibile rilevare un dispositivo e Impossibile gestire un dispositivo nella documentazione online di XClarity Administrator.

- La configurazione di rete deve consentire il traffico SLP tra XClarity Administrator e il dispositivo di storage rack.
- È necessario il protocollo SLP unicast.
- Affinché XClarity Administrator rilevi automaticamente i dispositivi Lenovo Storage, è richiesto il protocollo SLP multicast. Il protocollo SLP deve inoltre essere abilitato sul dispositivo di storage rack.

Informazioni su questa attività

XClarity Administrator può rilevare automaticamente i dispositivi di storage in un ambiente individuando i dispositivi gestibili che si trovano nella stessa sottorete IP di XClarity Administrator. Per rilevare i dispositivi di storage che si trovano in altre sottoreti, specificare un indirizzo IP o un intervallo di indirizzi IP oppure importare le informazioni da un foglio di calcolo.

Una volta gestiti i dispositivi di storage da parte di XClarity Administrator, XClarity Administrator esegue periodicamente il polling di ciascun dispositivo di storage gestito per raccogliere informazioni, quali inventario, VPD (Vital Product Data) e stato. È possibile visualizzare e monitorare ciascun dispositivo di storage gestito ed eseguire azioni di gestione (ad esempio, la configurazione delle impostazioni di sistema, l'aggiornamento del firmware, l'accensione e lo spegnimento).

Un dispositivo può essere gestito da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza iniziale di XClarity Administrator e quindi gestirlo con la

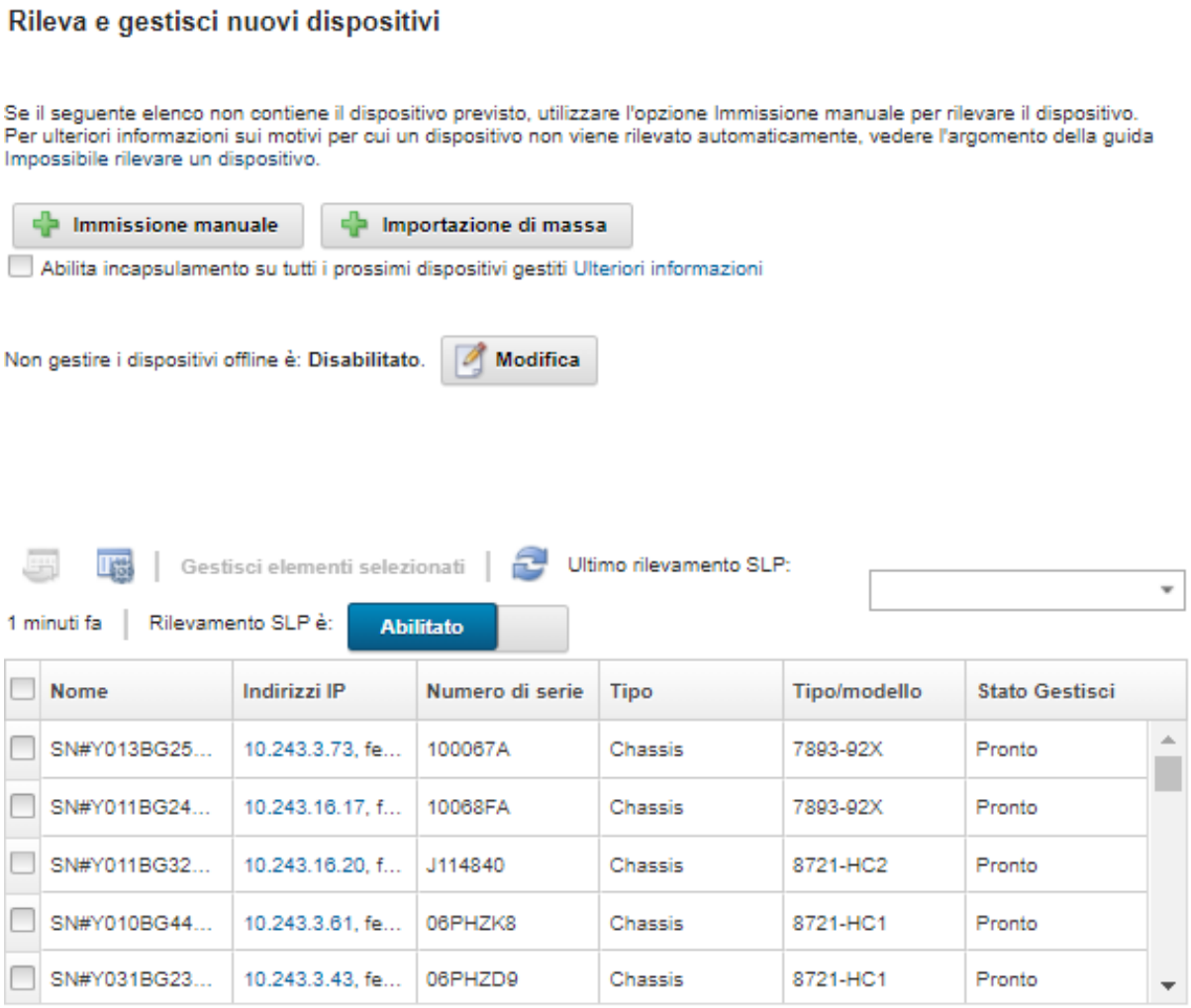
nuova istanza di XClarity Administrator. Se si verifica un errore durante il processo di annullamento della gestione, sarà possibile selezionare l'opzione **Forza gestione** durante la gestione nella nuova istanza di XClarity Administrator.

Nota: Quando si analizza la rete alla ricerca di dispositivi gestibili, XClarity Administrator non è in grado di sapere se un dispositivo è già gestito da un altro gestore fino a quando non avrà tentato di gestirlo.

Procedura

Completare una delle seguenti procedure per gestire i dispositivi di storage mediante XClarity Administrator.

- Rilevare e gestire un numero elevato di dispositivi di storage e altri tipi di dispositivi mediante un file di importazione di massa (vedere Gestione dei sistemi nella documentazione online di XClarity Administrator).
- Rilevare e gestire i dispositivi di storage che si trovano nella stessa sottorete IP di XClarity Administrator.
  1. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci nuovi dispositivi.



È possibile ordinare le colonne della tabella per individuare più facilmente i dispositivi di storage che si desidera gestire. Inoltre, è possibile immettere testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i sistemi di storage visualizzati. È possibile modificare le colonne visualizzate e l'ordinamento predefinito facendo clic sull'icona **Personalizza colonne** ( ).

2. Fare clic sull'icona **Aggiorna** () per rilevare tutti i dispositivi gestibili nel dominio di XClarity Administrator. Il rilevamento potrebbe richiedere diversi minuti.
3. Selezionare uno o più dispositivi di storage che si desidera gestire.
4. Fare clic su **Gestisci elementi selezionati**. Verrà visualizzata la finestra di dialogo Gestisci.
5. Specificare l'ID utente e la password per l'autenticazione con il dispositivo di storage.

   Suggerimento: per gestire il dispositivo si consiglia di utilizzare un account di supervisore o amministratore. Se viene utilizzato un account con autorità di livello inferiore, la gestione potrebbe avere esito negativo oppure potrebbe riuscire ma le altre operazioni XClarity Administrator future potrebbero non riuscire sul dispositivo (in particolar modo se il dispositivo viene gestito senza l'autenticazione gestita).
6. Fare clic su **Modifica** per modificare i gruppi di ruoli che devono essere assegnati ai dispositivi.

   Nota:

   – È possibile selezionare un elenco dei gruppi di ruoli assegnati all'utente corrente.
   – Se non si modificano i gruppi di ruoli, vengono utilizzati i gruppi di ruoli predefiniti. Per ulteriori informazioni sui gruppi di ruoli predefiniti, vedere Modifica delle autorizzazioni predefinite.
7. Fare clic su **Gestisci**.

   Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Per garantire il completamento del processo, monitorarne l'avanzamento.
8. Al termine del processo, fare clic su **OK**.

   Il dispositivo è ora gestito da XClarity Administrator, che effettua periodicamente il polling automatico del dispositivo gestito per raccogliere informazioni aggiornate, ad esempio l'inventario.

   Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione **Forza gestione**.

   – Se l'istanza XClarity Administrator di gestione è in errore e non è possibile effettuare il ripristino.

     Nota: se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabile) e l'opzione **Forza gestione**.
   – Se l'istanza XClarity Administrator di gestione è stata disattivata prima di avere annullato la gestione dei dispositivi.
   – Se la gestione dei dispositivi non è stata annullata correttamente.

   Attenzione: I dispositivi possono essere gestiti da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza originale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator.

- Per rilevare e gestire i dispositivi di storage che non si trovano nella stessa sottorete IP di XClarity Administrator, specificare manualmente gli indirizzi IP.
  1. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci.
  2. Selezionare **Immissione manuale**.
  3. Specificare gli indirizzi di rete dei dispositivi di storage che si desidera gestire:

     – Fare clic su **Singolo sistema** e immettere un singolo nome di dominio dell'indirizzo IP o il nome di dominio completo (FQDN).

Nota: Per specificare un FQDN, assicurarsi che nella pagina Accesso alla rete sia specificato un nome di dominio valido (vedere Configurazione dell'accesso alla rete).

- Fare clic su **Più sistemi** e immettere un intervallo indirizzi IP. Per aggiungere un altro intervallo, fare clic sull'icona **Aggiungi** (). Per rimuovere un intervallo, fare clic sull'icona **Rimuovi** ().

4. Fare clic su **OK**.
5. Specificare l'ID utente e la password per l'autenticazione con il dispositivo di storage.

   Suggerimento: per gestire il dispositivo si consiglia di utilizzare un account di supervisore o amministratore. Se viene utilizzato un account con autorità di livello inferiore, la gestione potrebbe avere esito negativo oppure potrebbe riuscire ma le altre operazioni XClarity Administrator future potrebbero non riuscire sul dispositivo (in particolar modo se il dispositivo viene gestito senza l'autenticazione gestita).
6. Fare clic su **Modifica** per modificare i gruppi di ruoli che devono essere assegnati ai dispositivi.

   Nota:

   - È possibile selezionare un elenco dei gruppi di ruoli assegnati all'utente corrente.
   - Se non si modificano i gruppi di ruoli, vengono utilizzati i gruppi di ruoli predefiniti. Per ulteriori informazioni sui gruppi di ruoli predefiniti, vedere Modifica delle autorizzazioni predefinite.
7. Fare clic su **Gestisci**.

   Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Per garantire il completamento del processo, monitorarne l'avanzamento.
8. Al termine del processo, fare clic su **OK**.

   Il dispositivo è ora gestito da XClarity Administrator, che effettua periodicamente il polling automatico del dispositivo gestito per raccogliere informazioni aggiornate, ad esempio l'inventario.

   Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione **Forza gestione**.

   - Se l'istanza XClarity Administrator di gestione è in errore e non è possibile effettuare il ripristino.

     Nota: se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabile) e l'opzione **Forza gestione**.
   - Se l'istanza XClarity Administrator di gestione è stata disattivata prima di avere annullato la gestione dei dispositivi.
   - Se la gestione dei dispositivi non è stata annullata correttamente.

   Attenzione: I dispositivi possono essere gestiti da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza originale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator.

Al termine

- Rilevare e gestire dispositivi aggiuntivi.
- Aggiornare il firmware sui dispositivi non conformi ai criteri correnti (vedere Aggiornamento del firmware sui dispositivi gestiti).
- Aggiungere i nuovi dispositivi al rack appropriato per riflettere l'ambiente fisico (vedere Gestione dei rack).
- Monitorare lo stato dell'hardware e i dettagli (vedere Visualizzazione dello stato dei dispositivi di storage).

- Monitorare eventi e avvisi (vedere Utilizzo degli eventi e Gestione degli avvisi).

Considerazioni sulla gestione dello storage

Prima di gestire un dispositivo di storage, valutare le seguenti considerazioni importanti.

Per informazioni sui requisiti delle porte, vedere Disponibilità della porta nella documentazione online di Lenovo XClarity Administrator.

Importante: Prima di rilevare e gestire i dispositivi di storage rack, verificare che i seguenti requisiti siano stati soddisfatti (diverso da ThinkSystem serie DE). Per ulteriori informazioni, vedere Impossibile rilevare un dispositivo e Impossibile gestire un dispositivo nella documentazione online di XClarity Administrator.

- La configurazione di rete deve consentire il traffico SLP tra XClarity Administrator e il dispositivo di storage rack.
- È necessario il protocollo SLP unicast.
- Affinché XClarity Administrator rilevi automaticamente i dispositivi Lenovo Storage, è richiesto il protocollo SLP multicast. Il protocollo SLP deve inoltre essere abilitato sul dispositivo di storage rack.

Per i dispositivi Lenovo Storage, la temperatura dell'aria a livello di sistema viene misurata in base al sensore di temperatura più vicino al midplane del sistema e riflette la temperatura ambiente in seguito all'attraversamento del flusso d'aria nelle unità. La temperatura dell'aria riportata da XClarity Administrator e quella riportata dal controller di gestione potrebbero differire se viene acquisita in momenti diversi.

Per i dispositivi di storage della serie Lenovo DE, entrambi i controller di gestione devono essere raggiungibili in rete durante la gestione iniziale.

Per alcuni dispositivi di storage, i trap SNMP sono solo in inglese.

Visualizzazione dello stato dei dispositivi di storage

Da Lenovo XClarity Administrator è possibile visualizzare un riepilogo e lo stato dettagliato dei dispositivi di storage gestiti.

Ulteriori informazioni:

- XClarity Administrator: inventario
- XClarity Administrator: monitoraggio

Informazioni su questa attività

Le seguenti icone di stato vengono utilizzate per indicare l'integrità complessiva del dispositivo. Se i certificati non corrispondono, "(Non attendibile)" viene aggiunto allo stato di ciascun dispositivo applicabile, ad esempio Avvertenza (non attendibile). Se si verifica un problema di connettività o una connessione al dispositivo non è attendibile, "(Connettività)" viene aggiunto allo stato di ciascun dispositivo applicabile, ad esempio Avvertenza (Connettività).

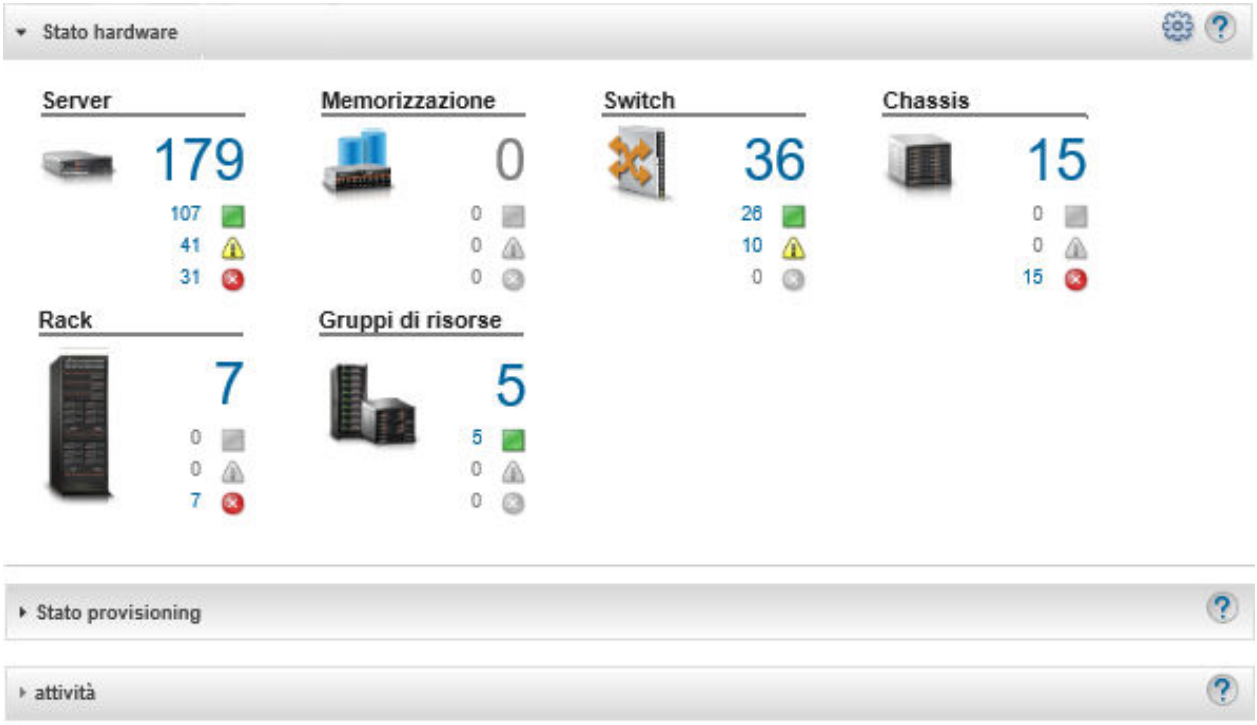
- ( ) Critico
- ( ) Avvertenza
- ( ) In sospeso
- ( ) Informativo
- ( ) Normale

- ( ) Offline
- ( ) Sconosciuto

Procedura

Per visualizzare lo stato di un dispositivo di storage gestito, effettuare una o più operazioni tra quelle riportate di seguito.

- Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Dashboard**. Verrà visualizzata la pagina Dashboard con una panoramica e lo stato di tutti i dispositivi di storage gestiti e delle altre risorse.



- Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware → Storage**. Verrà visualizzata la pagina Storage con una vista tabulare di tutti i dispositivi di storage installati nello chassis gestito.

  È possibile ordinare le colonne della tabella per individuare più facilmente i dispositivi di storage che si desidera gestire. Inoltre, è possibile immettere il testo (come il nome del sistema o l'indirizzo IP) nel campo **Filtro** e fare clic sulle icone di stato per elencare solo i dispositivi di storage che soddisfano i criteri selezionati.

Da questa pagina, è possibile eseguire le seguenti azioni:

- Visualizzare informazioni dettagliate sul dispositivo di storage e sui relativi componenti (vedere Visualizzazione dei dettagli di un dispositivo di storage).
- Visualizzare un dispositivo di storage nella vista grafica dello chassis o del rack facendo clic su **Tutte le azioni → Viste → Mostra nella vista rack** o **Tutte le azioni → Viste → Mostra nella vista chassis**.
- Avviare l'interfaccia Web del controller di gestione per il dispositivo di storage facendo clic sul collegamento **Indirizzo IP** (vedere Avvio dell'interfaccia del controller di gestione per un dispositivo di storage).
- Accendere e spegnere il controller di storage nel dispositivo di storage (vedere Accensione e spegnimento di un dispositivo di storage).
- Per modificare le informazioni di sistema, selezionare un dispositivo di storage e fare clic su **Tutte le azioni → Inventario → Modifica proprietà**.
- Per aggiornare l'inventario, selezionare un dispositivo di storage e fare clic su **Tutte le azioni → Inventario → Aggiorna inventario**.
- Esportare le informazioni dettagliate su uno o più dispositivi di storage in un unico file CSV selezionandoli e facendo clic su **Tutte le azioni → Inventario → Esporta inventario**.

  Nota: è possibile esportare i dati di inventario per un massimo di 60 dispositivi alla volta.

  Suggerimento: Durante l'importazione di un file CSV in Microsoft Excel, i valori di testo contenenti solo numeri vengono trattati come valori numerici (ad esempio nel caso degli UUID). Impostare la formattazione di ogni cella come testo per risolvere il problema.
- Annullare la gestione del dispositivo di storage (vedere Annullamento della gestione di un dispositivo di storage).
- Solo dispositivi di storage Flex System. Riposizionare virtualmente il controller di storage nel dispositivo di storage (vedere Riposizionamento virtuale dei controller di storage in un dispositivo di storage Flex System).
- Escludere gli eventi che non interessano l'utente da tutte le pagine in cui vengono visualizzati facendo clic sull'icona **Escludi eventi** (). (vedere Esclusione di eventi).
- Risolvere i problemi che potrebbero verificarsi tra il certificato di sicurezza di Lenovo XClarity Administrator e quello del modulo CMM nello chassis in cui è installato il dispositivo di storage selezionando un dispositivo di storage e facendo clic su **Tutte le azioni → Sicurezza → Risolvi certificati non attendibili** (vedere Risoluzione di un certificato server non attendibile).
- Aggiungere o rimuovere un dispositivo di storage da un gruppo di risorse statico facendo clic su **Tutte le azioni → Gruppi → Aggiungi a gruppo** o **Tutte le azioni → Gruppi → Rimuovi da gruppo**.

Visualizzazione dei dettagli di un dispositivo di storage

È possibile visualizzare informazioni dettagliate sui dispositivi di storage gestiti da Lenovo XClarity Administrator, tra cui indirizzo IP, nome del prodotto, numero di serie e dettagli su ciascun canister.

Informazioni su questa attività

Ulteriori informazioni:

-  XClarity Administrator: inventario
-  XClarity Administrator: monitoraggio

Per i dispositivi Lenovo Storage, la temperatura dell'aria a livello di sistema viene misurata in base al sensore di temperatura più vicino al midplane del sistema e riflette la temperatura ambiente in seguito all'attraversamento del flusso d'aria nelle unità. La temperatura dell'aria riportata da XClarity Administrator e quella riportata dal controller di gestione potrebbero differire se viene acquisita in momenti diversi.

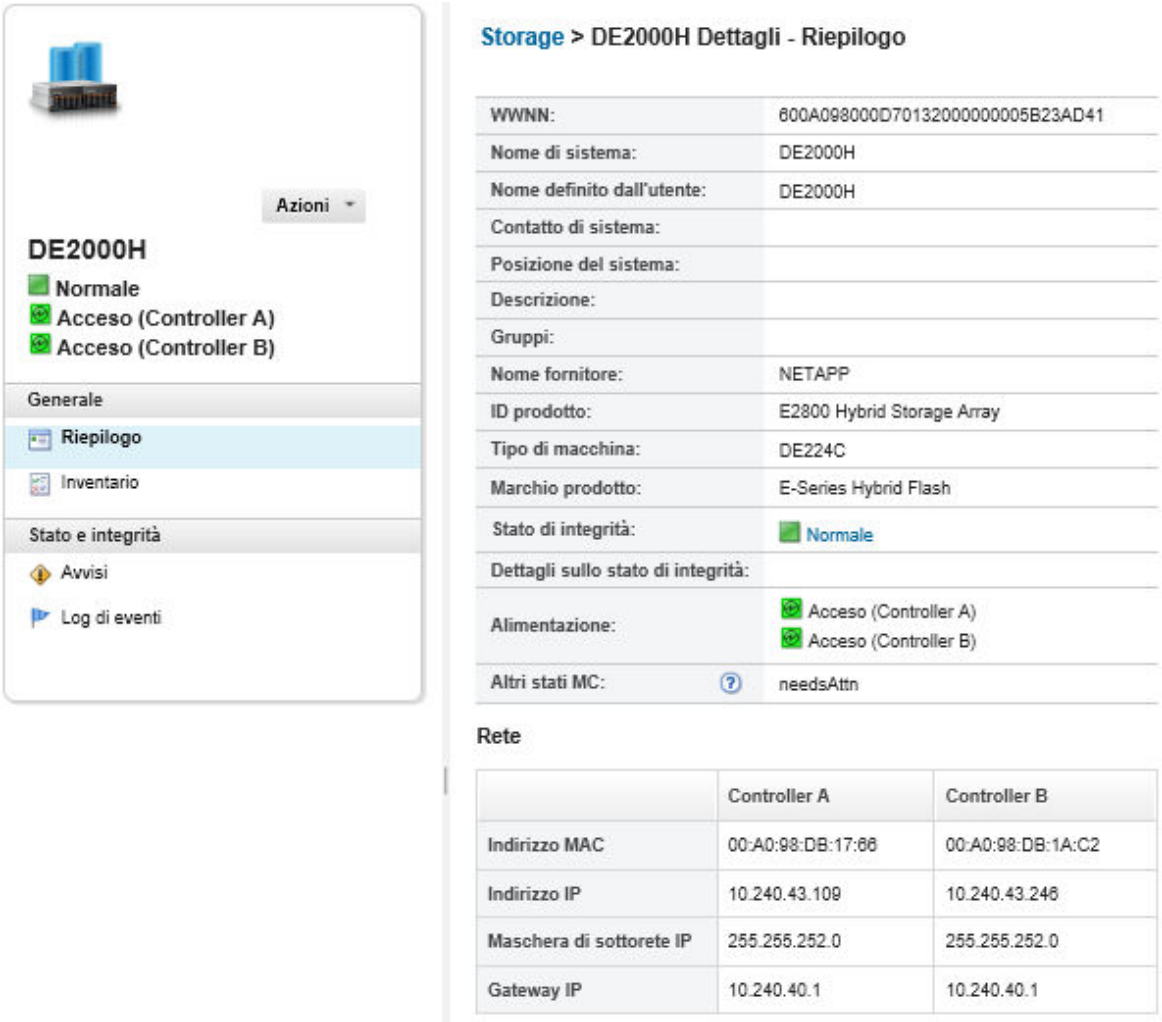
Procedura

Per visualizzare i dettagli di uno specifico dispositivo di storage gestito, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Storage**. Verrà visualizzata la pagina Storage con una vista tabulare di tutti i dispositivi di storage installati nello chassis gestito.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di specifici dispositivi di storage. Inoltre, immettere testo (ad esempio, nome del sistema o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i dispositivi di storage visualizzati.

Passo 2. Fare clic sul nome del dispositivo di storage nella colonna **Storage**. Verrà visualizzata la pagina di riepilogo che mostra le proprietà e un elenco dei componenti installati nel dispositivo di storage.



Passo 3. Completare una o più delle operazioni che seguono per visualizzare i dettagli dello storage. I dati visualizzati potrebbero differire in base al tipo di dispositivo di storage.

- Fare clic su **Riepilogo** per visualizzare un riepilogo del server e dei relativi componenti installati, che include le informazioni di sistema e i dispositivi installati (vedere Visualizzazione dello stato dei dispositivi di storage).
- Fare clic su **Dettagli inventario** per visualizzare i dettagli sui componenti del dispositivo di storage, tra cui:
  - Livelli di firmware per il dispositivo di storage.
  - Dettagli della rete del controller di gestione, ad esempio il nome host, l'indirizzo IPv4, l'indirizzo IPv6 e gli indirizzi MAC.
  - Dettagli delle risorse del dispositivo di storage.
  - Dettagli su ciascun canister nel dispositivo di storage.

  Suggerimento: se un nodo di espansione, ad esempio il nodo di espansione storage Flex System o il nodo PCIe Expansion Node Flex System, è installato nello chassis e connesso a uno dispositivo di storage, verranno visualizzati anche i relativi dettagli di inventario.
- Fare clic su **Avvisi** per visualizzare nel relativo elenco gli avvisi correlati al dispositivo di storage (vedere Gestione degli avvisi).
- Fare clic su **Log eventi** per visualizzare nel relativo log gli eventi correlati allo dispositivo di storage (vedere Utilizzo degli eventi).

- Fare clic su **Processi** per visualizzare un elenco di processi associati al dispositivo di storage (vedere Monitoraggio dei processi).
- Fare clic su **light path** per visualizzare lo stato corrente di ciascun LED sul dispositivo di storage.
- Fare clic su **Specifiche di alimentazione e termiche** per visualizzare le caratteristiche di alimentazione e termiche per il dispositivo di storage.

  Suggerimento: utilizzare il pulsante di aggiornamento nel browser Web per raccogliere i dati relativi alle specifiche di alimentazione e termiche più recenti. La raccolta dei dati potrebbe richiedere alcuni minuti.

Al termine

Oltre a visualizzare il riepilogo e le informazioni dettagliate su un dispositivo di storage, è possibile eseguire le seguenti operazioni:

- Visualizzare un dispositivo di storage nella vista grafica dello chassis o del rack facendo clic su **Azioni → Viste → Mostra nella vista rack** o **Azioni → Viste → Mostra nella vista chassis**.
- Esportare le informazioni dettagliate sul dispositivo di storage in un file CSV facendo clic su **Azioni → Inventario → Esporta inventario**.

  Nota:

  – Per ulteriori informazioni sui dati di inventario nel file CSV, vedere GET /storage/<*UUID_list*> API REST nella documentazione online di Lenovo XClarity Administrator.

  – Durante l'importazione di un file CSV in Microsoft Excel, i valori di testo contenenti solo numeri vengono trattati come valori numerici (ad esempio nel caso degli UUID). Impostare la formattazione di ogni cella come testo per risolvere il problema.
- Avviare l'interfaccia Web del controller di gestione per il dispositivo di storage facendo clic sul collegamento **Indirizzo IP** (vedere Avvio dell'interfaccia del controller di gestione per un dispositivo di storage).
- Accendere e spegnere un controller di storage nel dispositivo di storage (vedere Accensione e spegnimento di un dispositivo di storage).
- Riposizionare virtualmente il controller di storage nel dispositivo di storage (vedere Riposizionamento virtuale di un server in uno chassis di Flex System).
- Per modificare le informazioni di sistema, selezionare un dispositivo di storage e fare clic su **Modifica proprietà**.
- Per aggiornare l'inventario, selezionare un dispositivo di storage e fare clic su **Azioni → Inventario → Aggiorna inventario**.
- Escludere gli eventi che non interessano l'utente da tutte le pagine in cui vengono visualizzati facendo clic su **Azioni → Ripristino servizio → Escludi eventi** (vedere Esclusione di eventi).
- Risolvere i problemi che potrebbero verificarsi tra il certificato di sicurezza di XClarity Administrator e quello del modulo CMM nello chassis in cui è installato il dispositivo di storage selezionando un dispositivo di storage e facendo clic su **Azioni → Servizio → Risolvi certificati non attendibili** (vedere Risoluzione di un certificato server non attendibile).

Backup e ripristino dei dati di configurazione dello storage

Lenovo XClarity Administrator non include funzioni di backup integrate per i dati di configurazione dello storage. Utilizzare le funzioni di backup disponibili per il dispositivo d storage gestito.

Per informazioni sul ripristino del dispositivo, consultare la documentazione del prodotto fornita con il dispositivo di storage.

- Per i dispositivi Lenovo Storage, vedere Documentazione del prodotto Lenovo Storage S2200/S3200.
- Per i dispositivi di storage Lenovo ThinkSystem, vedere Documentazione del prodotto ThinkSystem Storage.

Accensione e spegnimento di un dispositivo di storage

È possibile accendere e spegnere un dispositivo di storage da Lenovo XClarity Administrator.

Informazioni su questa attività

Per i dispositivi di storage Flex System, quando un controller di storage è spento, in primo luogo i dati vengono memorizzati nell'unità, quindi il dispositivo di storage passa allo stato in standby. Nello stato in standby, i volumi forniti dal dispositivo di storage non sono più accessibili.

Per accendere un dispositivo di storage ThinkSystem serie DM, verificare che il controller di storage utilizzato per la gestione sia online e che il relativo indirizzo IP sia in grado di comunicare direttamente con il processore di servizio del controller di storage spento sulla rete esterna.

Procedura

Per accendere e spegnere un dispositivo di storage gestito, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Storage**. Verrà visualizzata la pagina Storage con una vista tabulare di tutti i dispositivi di storage installati nello chassis gestito.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di specifici dispositivi di storage. Inoltre, immettere testo (ad esempio, nome del sistema o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i dispositivi di storage visualizzati.

Passo 2. Selezionare il dispositivo di storage da accendere o spegnere.

Passo 3. Fare clic su **Tutte le azioni**, quindi selezionare una delle seguenti azioni di alimentazione:

- **Accendi controller A**
- **Accendi controller B**
- **Spegni controller A**
- **Spegni controller B**
- **Riavvia controller A**
- **Riavvia controller B**

Riposizionamento virtuale dei controller di storage in un dispositivo di storage Flex System

È possibile eseguire un riposizionamento virtuale, che simula la rimozione e il reinserimento di un controller di storage (canister) nel vano del dispositivo di storage

Informazioni su questa attività

Durante il riposizionamento virtuale, tutte le connessioni di rete esistenti al dispositivo di storage andranno perse e lo stato di alimentazione del dispositivo verrà modificato. Prima di eseguire un riposizionamento virtuale, accertarsi di aver salvato tutti i dati utente.

Procedura

Per riposizionare virtualmente un controller di storage, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware → Storage**. Verrà visualizzata la pagina Storage contenente una vista tabulare di tutti i dispositivi di storage.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di specifici dispositivi di storage. Inoltre, immettere testo (ad esempio, nome del sistema o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i dispositivi di storage visualizzati.

Passo 2. Selezionare il dispositivo di storage Flex System.

Passo 3. Fare clic su **Tutte le azioni → Servizio**, quindi su **Riposizionamento virtuale controller A** o **Riposizionamento virtuale controller B**.

Passo 4. Fare clic su **Riposizionamento virtuale**.

Avvio dell'interfaccia del controller di gestione per un dispositivo di storage

È possibile avviare l'interfaccia Web del controller di gestione per lo chassis in cui è installato il dispositivo di storage da Lenovo XClarity Administrator.

Procedura

Per avviare un'interfaccia Web del controller di gestione, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Storage**. Verrà visualizzata la pagina Storage contenente una vista tabulare di tutti i dispositivi di storage gestiti.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di specifici dispositivi di storage. Inoltre, immettere testo (ad esempio, nome del dispositivo o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i dispositivi di storage visualizzati.

Passo 2. Selezionare il dispositivo di storage.

Passo 3. Fare clic su **Azioni → Avvia → Interfaccia Web di gestione**. Verrà avviata l'interfaccia Web del controller di gestione.

Passo 4. Eseguire il login all'interfaccia del controller di gestione.

Nota: Per i dispositivi di storage Flex System, utilizzare le credenziali utente di XClarity Administrator.

Modifica delle proprietà di sistema per un dispositivo di storage

È possibile modificare le proprietà di sistema per un dispositivo di storage specifico.

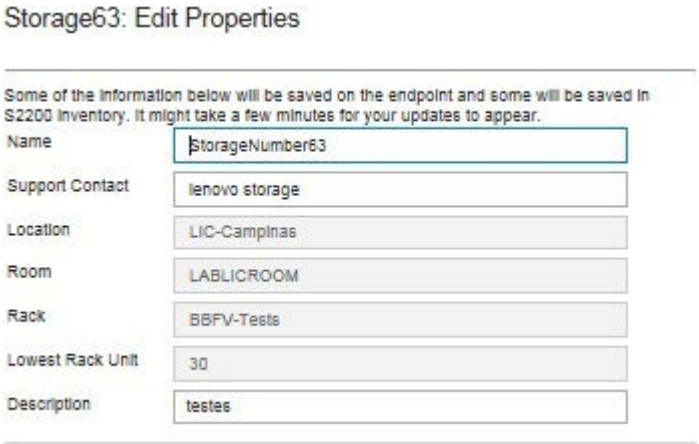
Procedura

Per modificare le proprietà di sistema, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Hardware → Storage** per visualizzare la pagina Storage.

Passo 2. Selezionare il dispositivo di storage da aggiornare.

Passo 3. Fare clic su **Tutte le azioni → Inventario → Modifica proprietà** per visualizzare la finestra di dialogo Modifica.



Passo 4. Modificare le seguenti informazioni, in base alle esigenze.
- Nome
- Contatto supporto

- Descrizione

Nota: XClarity Administrator aggiorna posizione, ambiente, rack e proprietà dell'unità inferiore del rack quando si aggiungono o rimuovono dispositivi da un rack nell'interfaccia Web (vedere Gestione dei rack).

Passo 5. Fare clic su **Salva**.

Nota: Quando vengono modificate queste proprietà, è possibile che si verifichi un breve ritardo nella visualizzazione delle modifiche nell'interfaccia Web di XClarity Administrator.

Ripristino della gestione di un dispositivo di storage rack dopo un errore del server di gestione

Se la gestione di un dispositivo di storage rack non è stata annullata correttamente, sarà necessario ripristinare il dispositivo di storage prima di poterne eseguire nuovamente la gestione. È possibile ripristinare la gestione cancellando parti specifiche della configurazione del dispositivo di storage precedentemente impostata da Lenovo XClarity Administrator.

Procedura

Per ripristinare un dispositivo di storage rack, attenersi alla procedura descritta di seguito.

- Se l'istanza di XClarity Administrator di sostituzione utilizza lo stesso indirizzo IP dell'istanza di XClarity Administrator con errori, è possibile gestire nuovamente il dispositivo utilizzando l'opzione **Forza gestione** (vedere Gestione di dispositivi di storage).
- Rimuovere tutti gli account utente con il prefisso "LXCA_" e facoltativamente rimuovere gli account utente con il prefisso "SYSMGR_" e il tipo "SNMPv3" dal dispositivo di storage.

Al termine

Una volta ripristinato o sostituito XClarity Administrator, il dispositivo di storage potrà essere nuovamente gestito (vedere Gestione di dispositivi di storage). Verranno mantenute tutte le informazioni sul dispositivo di storage (tra cui, le proprietà di sistema).

Ripristino della gestione di un dispositivo di storage Lenovo ThinkSystem serie DE dopo un errore del server di gestione

Se la gestione di un dispositivo di storage Lenovo ThinkSystem serie DE non è stata annullata correttamente, sarà necessario ripristinare il dispositivo di storage prima di poterne eseguire nuovamente la gestione. È possibile ripristinare la gestione cancellando parti specifiche della configurazione del dispositivo di storage precedentemente impostata da Lenovo XClarity Administrator.

Procedura

Per ripristinare un dispositivo di storage Lenovo ThinkSystem serie DE, attenersi alla procedura descritta di seguito.

- Se l'istanza di XClarity Administrator di sostituzione utilizza lo stesso indirizzo IP dell'istanza di XClarity Administrator con errori, è possibile gestire nuovamente il dispositivo utilizzando l'opzione **Forza gestione** (vedere Gestione di dispositivi di storage).
- Rimuovere la registrazione della coppia di chiavi "LXCA_REMOTE_MANAGMENT_VERIFICATION" dall'API della coppia di chiavi del dispositivo di storage.

Al termine

Una volta ripristinato o sostituito XClarity Administrator, il dispositivo di storage potrà essere nuovamente gestito (vedere Gestione di dispositivi di storage). Verranno mantenute tutte le informazioni sul dispositivo di storage (tra cui, le proprietà di sistema).

Annullamento della gestione di un dispositivo di storage

È possibile rimuovere un dispositivo di storage dalla gestione di Lenovo XClarity Administrator. Questo processo è detto *annullamento della gestione.*

Prima di iniziare

Prima di annullare la gestione di un dispositivo di storage, accertarsi che nello switch non siano in esecuzione processi attivi.

Informazioni su questa attività

Se si annulla la gestione di un dispositivo di storage, XClarity Administrator mantiene determinate informazioni sul dispositivo di storage. Queste informazioni verranno riapplicate quando lo stesso dispositivo di storage verrà nuovamente gestito.

Suggerimento: tutti i dispositivi dimostrativi aggiunti facoltativamente durante la configurazione iniziale sono nodi di uno chassis. Per annullare la gestione dei dispositivi dimostrativi, annullare la gestione dello chassis mediante l'opzione **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.

Procedura

Per annullare la gestione di un dispositivo di storage, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Hardware → Storage** per visualizzare la pagina Storage.

Passo 2. Selezionare uno o più dispositivi di storage dagli elenchi degli switch gestiti.

Passo 3. Fare clic su **Non gestire**. Viene visualizzata la finestra di dialogo Non gestire.

Passo 4. **Facoltativo:** selezionare **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.

Importante: quando si annulla la gestione di hardware dimostrativo, verificare di aver selezionato questa opzione.

Passo 5. Fare clic su **Non gestire**.La finestra di dialogo Non gestire mostra l'avanzamento di ogni operazione nel processo di annullamento della gestione.

Passo 6. Al termine del processo di annullamento della gestione, fare clic su **OK**.

Ripristino di un dispositivo di storage rack la cui gestione non è stata annullata correttamente

Se Lenovo XClarity Administrator gestisce un dispositivo di storage rack e si verificano errori in XClarity Administrator, è possibile ripristinare le funzioni di gestione finché il server di gestione non verrà ripristinato o sostituito. È possibile ripristinare la gestione del sistema cancellando parti specifiche della configurazione del dispositivo di storage precedentemente impostata da XClarity Administrator.

Procedura

Per ripristinare un dispositivo di storage rack, attenersi alla procedura descritta di seguito.

- Se l'istanza di XClarity Administrator di sostituzione utilizza lo stesso indirizzo IP dell'istanza di XClarity Administrator con errori, è possibile gestire nuovamente il dispositivo utilizzando l'opzione **Forza gestione** (vedere Gestione di dispositivi di storage).
- Rimuovere tutti gli account utente con il prefisso "LXCA_" e facoltativamente rimuovere gli account utente con il prefisso "SYSMGR_" e il tipo "SNMPv3" dal dispositivo di storage.

Al termine

Una volta ripristinato o sostituito XClarity Administrator, il dispositivo di storage potrà essere nuovamente gestito (vedere Gestione di dispositivi di storage). Verranno mantenute tutte le informazioni sul dispositivo di storage (tra cui, le proprietà di sistema).

Capitolo 10. Gestione degli switch

Lenovo XClarity Administrator è in grado di gestire gli switch di rete.

Ulteriori informazioni:

- XClarity Administrator: rilevamento
- XClarity Administrator: gestione degli switch

Prima di iniziare

Attenzione: Prima di gestire uno switch, osservare le relative considerazioni di gestione. Per informazioni, vedere Considerazioni sulla gestione degli switch.

Nota: Gli switch Flex vengono rilevati e gestiti automaticamente quando si gestisce lo chassis che li contiene. Non è possibile rilevare e gestire switch Flex indipendenti da uno chassis.

Alcune porte devono essere disponibili per la comunicazione con gli switch. Accertarsi che tutte le porte necessarie siano disponibili prima di gestire uno switch. Per informazioni sulle porte, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.

Accertarsi che sia installato il firmware minimo richiesto in ciascuno switch che si desidera gestire mediante XClarity Administrator. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.

Prima di gestire gli switch rack, verificare che siano state create le credenziali memorizzate in XClarity Administrator. XClarity Administrator utilizza solo le credenziali memorizzate per autenticare gli switch rack. Le credenziali memorizzate devono corrispondere a un account utente attivo sul dispositivo. È possibile creare le credenziali memorizzate dalle finestre di dialogo di gestione o dalla pagina "Credenziali memorizzate". Per ulteriori informazioni, vedere Gestione delle credenziali memorizzate.

La gestione mediante le interfacce loopback è supportata per tutti i dispositivi RackSwitch. Verificare che XClarity Administrator sia collegato all'interfaccia loopback, aggiungendo un instradamento statico o annunciando l'indirizzo tramite un protocollo di instradamento. Tenere presente che l'instradamento non può essere eseguito tra la porta di gestione e *qualsiasi* porta dati (come loopback).

Per gli switch Lenovo ThinkSystem serie DB:

- è necessario FOS 8.2.3 o versione successiva
- Accertarsi di configurare l'utente SNMPv3 all'indice 1 sullo switch *prima* di gestire lo switch utilizzando il seguente comando sullo switch: `snmpconfig --add snmpv3 -index 1 -user snmpadmin1 -groupname rw`
- Accertarsi che nello switch sia abilitato il protocollo REST. Per abilitare REST, utilizzare il comando seguente: `mgmtapp --enable rest`
- Verificare che il numero di sessioni REST consentite sia 10. Per impostare il numero di sessioni REST, utilizzare il seguente comando: `mgmtapp --config -maxrestsession 10`
- Gli switch Lenovo ThinkSystem serie DB non sono rilevabili mediante i protocolli di rilevamento dei servizi. Per gestire questi switch, utilizzare l'opzione **Immissione manuale**, clear **Protocolli di rilevamento dei servizi utente per identificare il tipo di dispositivo**, quindi selezionare "Switch Lenovo ThinkSystem serie DB" dall'elenco **Tipo di dispositivo**. Per ulteriori dettagli, consultare la procedura seguente sul rilevamento e la gestione degli switch che non si trovano nella stessa sottorete IP di XClarity Administrator.

Per gli switch NVIDIA:

- è necessario Cumulus 4.3 o versione successiva
- Gli switch NVIDIA non sono rilevabili mediante i protocolli di rilevamento dei servizi. Per gestire questi switch, utilizzare l'opzione **Immissione manuale**, cancellare Protocolli di rilevamento dei servizi utente per identificare il tipo di dispositivo, quindi selezionare "Switch NVIDIA" dall'elenco **Tipo di dispositivo**. Per ulteriori dettagli, vedere la procedura seguente sul rilevamento e la gestione degli switch che non si trovano nella stessa sottorete IP di XClarity Administrator.

Informazioni su questa attività

XClarity Administrator può rilevare automaticamente gli switch RackSwitch in un ambiente individuando i dispositivi gestibili che si trovano nella stessa sottorete IP di XClarity Administrator. Per rilevare gli switch che si trovano in altre sottoreti, specificare un indirizzo IP o un intervallo di indirizzi IP oppure importare le informazioni da un foglio di calcolo.

Nota: Le credenziali manuali non sono supportati per gli switch rack in XClarity Administrator.

Una volta gestiti gli switch da parte di XClarity Administrator, XClarity Administrator esegue periodicamente il polling di ciascuno switch gestito per raccogliere informazioni, quali inventario, VPD (Vital Product Data) e stato. È possibile visualizzare e monitorare ogni switch gestito ed eseguire attività di gestione, quali l'avvio della console di gestione, l'accensione e lo spegnimento.

Se XClarity Administrator perde la comunicazione con lo switch (ad esempio, a causa di un'interruzione dell'alimentazione, di un errore di rete o se lo switch è offline) durante la raccolta dell'inventario nel processo di gestione, la gestione viene completata correttamente. Tuttavia, alcune informazioni di inventario potrebbero essere incomplete. Attendere che lo switch torni online e che XClarity Administrator esegua il polling dello switch per l'inventario oppure raccogliere manualmente l'inventario sullo switch dalla pagina "Switch" selezionando lo switch e facendo clic su **Tutte le azioni → Inventario → Aggiorna inventario**.

Nota: Gli switch possono essere impilati. Uno *switch impilato* è un gruppo di switch che funziona come switch di rete singolo. Lo stack include uno *switch master* e uno o più *switch membro*. Per gli switch Flex, è possibile visualizzare e monitorare ciascuno switch nello stack e raccogliere dati diagnostici; tuttavia, non è possibile eseguire attività di gestione (tra cui aggiornamenti firmware e configurazione del server) in uno switch impilato. Queste attività di gestione di XClarity Administrator sono disabilitate per tutti gli switch impilati, incluso lo switch master. È possibile aggiornare il firmware nello switch impilato direttamente dalla CLI dello switch master. Per gli switch RackSwitch è possibile visualizzare e monitorare solo le informazioni sullo switch master. Gli switch membri non vengono rilevati da XClarity Administrator.

Le attività di gestione sono disabilitate anche per gli Switch Flex in modalità protetta.

Un dispositivo può essere gestito da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza iniziale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator. Se si verifica un errore durante il processo di annullamento della gestione, sarà possibile selezionare l'opzione **Forza gestione** durante la gestione nella nuova istanza di XClarity Administrator.

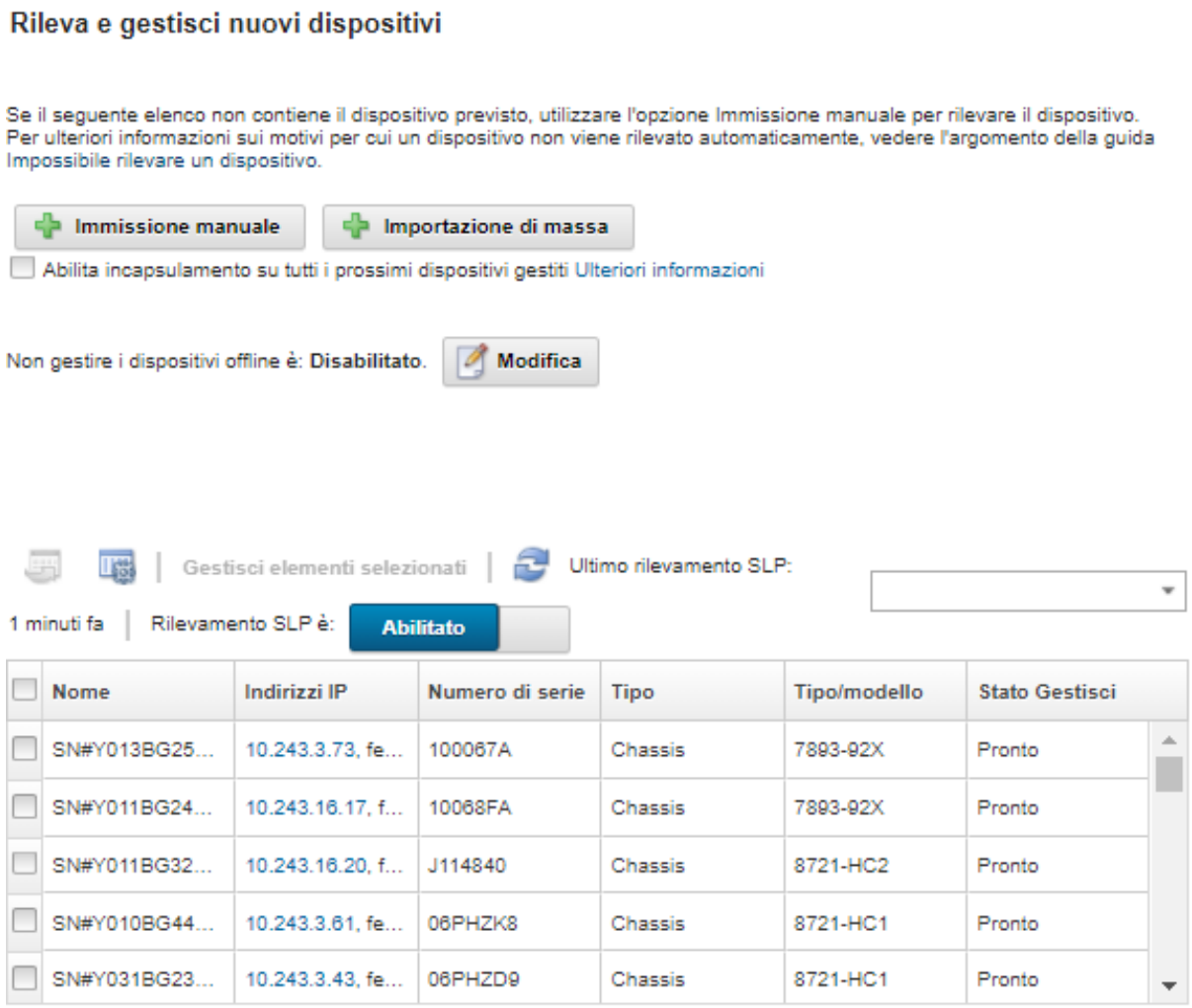
Nota: Quando si analizza la rete alla ricerca di dispositivi gestibili, XClarity Administrator non è in grado di sapere se un dispositivo è già gestito da un altro gestore fino a quando non avrà tentato di gestirlo.

Se uno switch è gestito direttamente mediante SSH o indirettamente mediante un modulo CMM, lo switch viene identificato come gestito da XClarity Administrator, viene eseguita la configurazione necessaria per l'interazione e viene raccolto l'inventario.

Procedura

Per gestire gli switch RackSwitch mediante XClarity Administrator, effettuare una delle seguenti procedure.

- Rilevare e gestire un numero elevato di switch e altri dispositivi tramite un file di importazione di massa (vedere Gestione dei sistemi nella documentazione online di Lenovo XClarity Administrator).
- Rilevare e gestire gli switch RackSwitch che si trovano nella stessa sottorete IP di XClarity Administrator.
  1. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci nuovi dispositivi.



     È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. È inoltre possibile immettere testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati. È possibile modificare le colonne visualizzate e l'ordinamento predefinito facendo clic sull'icona **Personalizza colonne** ( ).
  2. Fare clic sull'icona **Aggiorna** ( ) per rilevare tutti i dispositivi gestibili nel dominio di XClarity Administrator. Il rilevamento potrebbe richiedere diversi minuti.
  3. Selezionare uno o più switch che si desidera gestire.
  4. Fare clic su **Gestisci elementi selezionati**.
  5. Specificare le credenziali memorizzate per l'autenticazione con gli switch.

Suggerimento:

- Fare clic su **Gestisci credenziali memorizzate** per creare e gestire le credenziali memorizzate in XClarity Administrator (vedere Gestione delle credenziali memorizzate).
- Per gestire il dispositivo si consiglia di utilizzare un account di supervisore o amministratore. Se viene utilizzato un account con autorità di livello inferiore, la gestione potrebbe avere esito negativo oppure potrebbe riuscire ma le altre operazioni XClarity Administrator future potrebbero non riuscire sul dispositivo (in particolar modo se il dispositivo viene gestito senza l'autenticazione gestita).

6. (Solo switch che eseguono ENOS). Se impostata, specificare la password "enable" utilizzata per accedere alla modalità di esecuzione con privilegi nello switch.

   Quando si gestisce uno switch RackSwitch che esegue ENOS, è richiesto l'accesso alla modalità di esecuzione con privilegi sullo switch. Viene utilizzata da XClarity Administrator in caso di emissione del comando "enable" nello switch. Per impostazione predefinita, non è impostata alcuna password per questo comando sullo switch. Se tuttavia l'amministratore dello switch ha configurato una password per questo comando per incrementare il livello di sicurezza, deve essere specificata per garantire la gestione corretta dello switch da parte di XClarity Administrator.

7. Facoltativo: (solo per gli switch che eseguono ENOS) scegliere se abilitare HTTPS sullo switch facendo clic su **Avanzate** e quindi selezionando **Abilita HTTPS**. Questa opzione è abilitata per impostazione predefinita.

   Nota:

   - Per gli switch che eseguono CNOS, HTTPS deve essere abilitato sullo switch prima della gestione (vedere Considerazioni sulla gestione degli switch).
   - Se si sceglie di non abilitare HTTPS, viene utilizzata l'impostazione corrente sullo switch.
   - Quando viene annullata la gestione dello switch, XClarity Administrator ripristina l'impostazione HTTPS originale.

8. Facoltativo: scegliere se sostituire la configurazione NTP sullo switch con le impostazioni di configurazione NTP e fuso orario definite per Lenovo XClarity Administrator facendo clic su **Avanzate** e quindi selezionando **Configura i client NTP per utilizzare le impostazioni NTP dal server di gestione**. Questa opzione è abilitata per impostazione predefinita.

   Nota:

   - Se si sceglie di *non* sostituire la configurazione NTP e il fuso orario, la data e l'ora per le voci di log e gli eventi potrebbero non essere sincronizzate tra switch gestito e server di gestione.
   - Quando viene annullata la gestione dello switch, XClarity Administrator ripristina le impostazioni originali di configurazione NTP e fuso orario.

9. Fare clic su **Modifica** per modificare i gruppi di ruoli che devono essere assegnati ai dispositivi.

   Nota:

   - È possibile selezionare un elenco dei gruppi di ruoli assegnati all'utente corrente.
   - Se non si modificano i gruppi di ruoli, vengono utilizzati i gruppi di ruoli predefiniti. Per ulteriori informazioni sui gruppi di ruoli predefiniti, vedere Modifica delle autorizzazioni predefinite.

10. Fare clic su **Gestisci**.

    Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Per garantire il completamento del processo, monitorarne l'avanzamento.

11. Al termine del processo, fare clic su **OK**.

    Il dispositivo è ora gestito da XClarity Administrator, che effettua periodicamente il polling automatico del dispositivo gestito per raccogliere informazioni aggiornate, ad esempio l'inventario.

Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione **Forza gestione**.

- Se l'istanza XClarity Administrator di gestione è in errore e non è possibile effettuare il ripristino.

  Nota: se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabile) e l'opzione **Forza gestione**.
- Se l'istanza XClarity Administrator di gestione è stata disattivata prima di avere annullato la gestione dei dispositivi.
- Se la gestione dei dispositivi non è stata annullata correttamente.

Attenzione: I dispositivi possono essere gestiti da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza originale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator.

- Per rilevare e gestire gli switch RackSwitch che non si trovano nella stessa sottorete IP di XClarity Administrator, specificare manualmente gli indirizzi IP:
  1. Dalla barra di menu di Lenovo XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci.
  2. Selezionare **Immissione manuale**.
  3. Specificare gli indirizzi di rete degli switch che si desidera gestire:
     - Fare clic su **Singolo sistema** e immettere un singolo nome di dominio dell'indirizzo IP o il nome di dominio completo (FQDN).

       Nota: Per specificare un FQDN, assicurarsi che nella pagina Accesso alla rete sia specificato un nome di dominio valido (vedere Configurazione dell'accesso alla rete).
     - Fare clic su **Più sistemi** e immettere un intervallo indirizzi IP. Per aggiungere un altro intervallo, fare clic sull'icona **Aggiungi** (). Per rimuovere un intervallo, fare clic sull'icona **Rimuovi** ().
  4. Se il tipo di dispositivo non è individuabile utilizzando i protocolli di rilevamento dei servizi, cancellare i protocolli di rilevamento del servizio utente per identificare il tipo di dispositivo e quindi selezionare il tipo di dispositivo da gestire nell'elenco a discesa.

     I protocolli di rilevamento dei servizi, ad esempio SLP e SSDP, consentono di individuare automaticamente il tipo di dispositivo XClarity Administrator che sta per essere gestito e quindi di utilizzare il meccanismo appropriato per gestire il dispositivo. Alcuni tipi di dispositivo non supportano i protocolli di rilevamento dei servizi e in alcuni ambienti i protocolli di rilevamento dei servizi sono disattivati specificamente. In entrambi i casi, è necessario scegliere il tipo di dispositivo appropriato per completare il processo di gestione. I tipi di dispositivo seguenti devono essere identificati in modo esplicito.
     - Switch Lenovo ThinkSystem serie DB
     - Switch NVIDIA Mellanox
  5. Fare clic su **OK**.
  6. Specificare le credenziali memorizzate per l'autenticazione con gli switch.

     Suggerimento:

     - Fare clic su **Gestisci credenziali memorizzate** per creare e gestire le credenziali memorizzate in XClarity Administrator (vedere Gestione delle credenziali memorizzate).
     - Per gestire il dispositivo si consiglia di utilizzare un account di supervisore o amministratore. Se viene utilizzato un account con autorità di livello inferiore, la gestione potrebbe avere esito negativo

oppure potrebbe riuscire ma le altre operazioni XClarity Administrator future potrebbero non riuscire sul dispositivo (in particolar modo se il dispositivo viene gestito senza l'autenticazione gestita).

7. (Solo switch che eseguono ENOS). Se impostata, specificare la password "enable" utilizzata per accedere alla modalità di esecuzione con privilegi nello switch.

   Quando si gestisce uno switch RackSwitch che esegue ENOS, è richiesto l'accesso alla modalità di esecuzione con privilegi sullo switch. Viene utilizzata da XClarity Administrator in caso di emissione del comando "enable" nello switch. Per impostazione predefinita, non è impostata alcuna password per questo comando sullo switch. Se tuttavia l'amministratore dello switch ha configurato una password per questo comando per incrementare il livello di sicurezza, deve essere specificata per garantire la gestione corretta dello switch da parte di XClarity Administrator.

8. Facoltativo: (solo per gli switch che eseguono ENOS) scegliere se abilitare HTTPS sullo switch facendo clic su **Avanzate** e quindi selezionando **Abilita HTTPS**. Questa opzione è abilitata per impostazione predefinita.

   Nota:

   - Per gli switch che eseguono CNOS, HTTPS deve essere abilitato sullo switch prima della gestione (vedere Considerazioni sulla gestione degli switch).
   - Se si sceglie di non abilitare HTTPS, viene utilizzata l'impostazione corrente sullo switch.
   - Quando viene annullata la gestione dello switch, XClarity Administrator ripristina l'impostazione HTTPS originale.

9. Facoltativo: scegliere se sostituire la configurazione NTP sullo switch con le impostazioni di configurazione NTP e fuso orario definite per Lenovo XClarity Administrator facendo clic su **Avanzate** e quindi selezionando **Configura i client NTP per utilizzare le impostazioni NTP dal server di gestione**. Questa opzione è abilitata per impostazione predefinita.

   Nota:

   - Se si sceglie di *non* sostituire la configurazione NTP e il fuso orario, la data e l'ora per le voci di log e gli eventi potrebbero non essere sincronizzate tra switch gestito e server di gestione.
   - Quando viene annullata la gestione dello switch, XClarity Administrator ripristina le impostazioni originali di configurazione NTP e fuso orario.

10. Fare clic su **Modifica** per modificare i gruppi di ruoli che devono essere assegnati ai dispositivi.

    Nota:

    - È possibile selezionare un elenco dei gruppi di ruoli assegnati all'utente corrente.
    - Se non si modificano i gruppi di ruoli, vengono utilizzati i gruppi di ruoli predefiniti. Per ulteriori informazioni sui gruppi di ruoli predefiniti, vedere Modifica delle autorizzazioni predefinite.

11. Fare clic su **Gestisci**.

    Verrà visualizzata una finestra di dialogo che mostra l'avanzamento di questo processo di gestione. Per garantire il completamento del processo, monitorarne l'avanzamento.

12. Al termine del processo, fare clic su **OK**.

    Il dispositivo è ora gestito da XClarity Administrator, che effettua periodicamente il polling automatico del dispositivo gestito per raccogliere informazioni aggiornate, ad esempio l'inventario.

    Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione **Forza gestione**.

    - Se l'istanza XClarity Administrator di gestione è in errore e non è possibile effettuare il ripristino.

Nota: se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabile) e l'opzione **Forza gestione**.

- Se l'istanza XClarity Administrator di gestione è stata disattivata prima di avere annullato la gestione dei dispositivi.
- Se la gestione dei dispositivi non è stata annullata correttamente.

Attenzione: I dispositivi possono essere gestiti da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza originale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator.

Al termine

- Rilevare e gestire dispositivi aggiuntivi.
- Aggiungere i nuovi dispositivi gestiti al rack appropriato per riflettere l'ambiente fisico (vedere Gestione dei rack).
- Monitorare lo stato dell'hardware e i dettagli (vedere Visualizzazione dello stato degli switch).
- Monitorare gli eventi (vedere Utilizzo degli eventi).

Considerazioni sulla gestione degli switch

Prima di gestire uno switch, valutare le seguenti considerazioni importanti.

Per informazioni sui requisiti delle porte, vedere Disponibilità della porta nella documentazione online di Lenovo XClarity Administrator.

I dispositivi RackSwitch possono essere gestiti tramite la porta di gestione o una delle porte dati. I dispositivi RackSwitch con CNOS possono essere gestiti solo su interfacce che appartengono al VRF di "gestione" o "predefinito".

Nota: La gestione dei dispositivi RackSwitch utilizzando il collegamento locale IPv6 mediante una porta dati o una porta di gestione non è supportata.

Configurazione di eventi XClarity e trap SNMP

Quando viene gestito un dispositivo RackSwitch che esegue ENOS (qualsiasi versione), l'origine trap SNMP è impostata sull'interfaccia con l'indirizzo IP utilizzato per la gestione.

Quando viene gestito un dispositivo RackSwitch che esegue CNOS v10.8.1 o versioni successive, il VRF con origine trap SNMP viene verificato e modificato in modo da corrispondere alla porta utilizzata per la gestione.

Per i dispositivi RackSwitch che eseguono versioni precedenti alla 10.8.1 di CNOS, XClarity Administrator richiede l'origine trap SNMP al VRF collegato alla porta utilizzata per la gestione. Il valore predefinito "tutto" consente di utilizzare le porte dati o di gestione. Se la configurazione dello switch non utilizza il valore predefinito, deve essere modificata in modo da corrispondere alla porta utilizzata per la gestione.

- Se la porta di gestione viene utilizzata per la gestione, impostare il VFR con origine trap SNMP su "tutto" o "gestione".
- Se una delle porte dati viene utilizzata per la gestione, impostare il VFR con origine trap SNMP su "tutto" o "predefinito".

Switch RackSwitch che eseguono CNOS

HTTPS deve essere abilitato per la gestione e SLP deve essere abilitato per il rilevamento.

Nota: HTTPS è abilitato per impostazione predefinita su CNOS. Se la configurazione predefinita di restApi è stata modificata (utilizzando il comando `feature restApi http`), è possibile reimpostarla su HTTPS mediante il comando `feature restApi`. Per controllare lo stato corrente, utilizzare il comando `display restApi server` L'output riflette lo stato corrente. Se il numero di porta è seguito da "(HTTP)", significa che HTTPS è *disabilitato* . In caso contrario, la porta deve essere 443.

Quando viene annullata la gestione di un dispositivo RackSwitch, XClarity Administrator potrebbe non essere in grado di ripristinare l'opzione "pref." con il valore precedente alla gestione del dispositivo, a seconda della versione del firmware CNOS.

Switch RackSwitch che eseguono ENOS

- Se gli switch RackSwitch si trovano su una rete diversa da XClarity Administrator, la rete deve essere configurata per consentire il protocollo UDP in ingresso attraverso le porte 161 e 162, in modo che XClarity Administrator possa ricevere eventi e gestire tali dispositivi.
- SSH deve essere abilitato per la gestione e SLP deve essere abilitato per il rilevamento. HTTPS è facoltativo. Tuttavia, deve essere abilitato per avviare l'interfaccia web dello switch
- A seconda della versione del firmware dello switch RackSwitch, potrebbe essere necessario abilitare manualmente l'inoltro SLP multicast e il protocollo SSH su ogni switch RackSwitch utilizzando i seguenti comandi prima che lo switch possa essere rilevato e gestito da XClarity Administrator. Per ulteriori informazioni, vedere le Switch rack nella documentazione online di System x.
  - `ip slp enable`
  - `ssh enable`
- Quando viene gestito uno switch RackSwitch, XClarity Administrator modifica le seguenti impostazioni di configurazione. La modifica di tali impostazioni su uno switch gestito potrebbe interrompere la connettività e impedire l'esecuzione di determinate azioni di gestione. Quando viene annullata la gestione di uno switch RackSwitch, le impostazioni di configurazione vengono ripristinate ai valori originali (prima della gestione).
  - snmp-server access 32
  - snmp-server group 16
  - snmp-server notify 16
  - snmp-server target-parameters 16
  - snmp-server target-address 16
  - snmp-server trap-source <*IP interface*>
  - snmp-server user 16
  - versione snmp-server <*v3only or v1v2v3*>
  - ntp enable
  - ntp primary-server <*hostname or IP address*> MGT
  - ntp secondary-server <*hostname or IP address*> MGT
  - ntp interval 1500
  - ntp offset 500
  - access https enable

  È possibile utilizzare XClarity Administrator per regolare le seguenti impostazioni di configurazione modificando le informazioni di contatto del supporto, il nome o le proprietà di posizione per lo switch. La posizione verrà modificata all'aggiunta dello switch a un rack.
  - hostname "<*device_name*>"
  - snmp-server location "Location:<*location*>,Room:<*room*>,Rack:<*rack*>,LRU:<*lru*>"
  - snmp-server contact "<*contact_name*>"

Visualizzazione dello stato degli switch

È possibile visualizzare lo stato di tutti gli switch gestiti da Lenovo XClarity Administrator.

Ulteriori informazioni:

- XClarity Administrator: inventario
- XClarity Administrator: monitoraggio

Informazioni su questa attività

Le seguenti icone di stato vengono utilizzate per indicare l'integrità complessiva del dispositivo. Se i certificati non corrispondono, "(Non attendibile)" viene aggiunto allo stato di ciascun dispositivo applicabile, ad esempio Avvertenza (non attendibile). Se si verifica un problema di connettività o una connessione al dispositivo non è attendibile, "(Connettività)" viene aggiunto allo stato di ciascun dispositivo applicabile, ad esempio Avvertenza (Connettività).

- ( ) Critico
  - Uno o più sensori di temperatura rientrano nell'intervallo di guasti.
  - Le ventole o i moduli delle ventole non funzionano, come riportato di seguito:
    - RackSwitch G8124-E: una o più ventole sono in funzione a una velocità inferiore o pari a 100 RPM.
    - RackSwitch G8052: meno di tre moduli delle ventole sono in buono stato. Se le ventole in tale modulo sono in funzione a una velocità superiore a 500 RPM, un modulo viene considerato in buono stato.
    - RackSwitch G8264, G8264CS, G8332, G8272: meno di quattro moduli delle ventole sono in buono stato. Se le ventole in tale modulo sono in funzione a una velocità superiore a 500 RPM, un modulo viene considerato in buono stato.
    - RackSwitch G8296: meno di tre moduli delle ventole sono in buono stato. Se le ventole in tale modulo sono in funzione a una velocità superiore a 480 RPM, un modulo viene considerato in buono stato.
    - RackSwitch G7028, G7052: meno di tre moduli delle ventole sono in buono stato. Se le ventole in tale modulo sono in funzione a una velocità superiore a 500 RPM, un modulo viene considerato in buono stato.
  - Un alimentatore è spento.
- ( ) Avvertenza
  - Uno o più sensori di temperatura rientrano nell'intervallo di avvertenza.
  - Nel flash è stato rilevato un errore grave del dump.
- ( ) In sospeso
- ( ) Informativo
- ( ) Normale
  - Tutti i sensori di temperatura rientrano nell'intervallo normale.
  - Tutte le ventole o i moduli delle ventole funzionano.
  - Entrambi gli alimentatori sono accesi.
  - Non è stato rilevato alcun errore grave del dump.
- ( ) Offline
- ( ) Sconosciuto

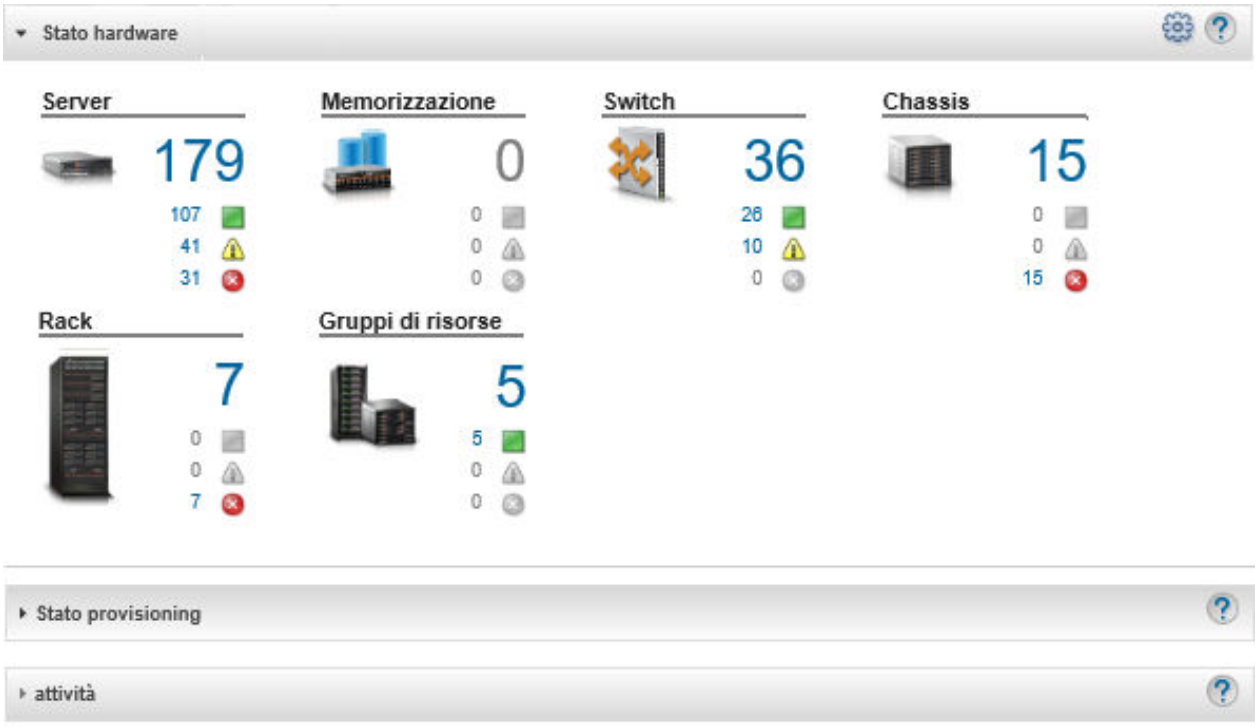
Un dispositivo può trovarsi in uno dei seguenti stati di alimentazione:
- Attivato
- Disattivato
- Arresto di

- Standby
- Iberna
- Unknown

Procedura

Per visualizzare lo stato di uno switch gestito, effettuare una o più operazioni tra quelle riportate di seguito.

- Dalla barra dei menu di XClarity Administrator, fare clic su **Dashboard**. Verrà visualizzata la pagina Dashboard con una panoramica e lo stato di tutti gli switch gestiti e delle altre risorse.



- Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch contenente una vista tabulare di tutti gli switch gestiti.

  È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. Inoltre, è possibile immettere il testo (come un nome o l'indirizzo IP) nel campo **Filtro** e fare clic sulle icone di stato per elencare solo gli switch che soddisfano i criteri selezionati.

Da questa pagina, è possibile eseguire le seguenti azioni:

- Visualizzare informazioni dettagliate sullo switch (vedere Visualizzazione dei dettagli di uno switch).
- Visualizzare uno switch Flex nella vista grafica dello chassis o del rack facendo clic su **Tutte le azioni → Viste → Mostra nella vista rack** o **Tutte le azioni → Viste → Mostra nella vista chassis**.
- Visualizzare uno switch RackSwitch nella vista rack grafica facendo clic su **Tutte le azioni → Viste → Mostra nella vista rack**.
- Avviare l'interfaccia Web del controller di gestione per lo switch facendo clic sul collegamento **Indirizzo IP** (vedere Avvio dell'interfaccia del controller di gestione per uno switch).
- Avviare la console SSH dello switch (vedere Avvio di una sessione SSH remota per uno switch).
- Accendere e spegnere lo switch (vedere Accensione e spegnimento di uno switch).
- Solo switch RackSwitch. Modificare le informazioni di sistema selezionando uno switch e facendo clic su **Tutte le azioni → Inventario → Modifica proprietà**.
- Per aggiornare l'inventario, selezionare un server e fare clic su **Tutte le azioni → Inventario → Aggiorna inventario**.
- Esportare le informazioni dettagliate su uno o più switch in un unico file CSV selezionando gli switch e facendo clic su **Tutte le azioni → Inventario → Esporta inventario** (vedere Esclusione di eventi).

  Nota: è possibile esportare i dati di inventario per un massimo di 60 dispositivi alla volta.

  Suggerimento: Durante l'importazione di un file CSV in Microsoft Excel, i valori di testo contenenti solo numeri vengono trattati come valori numerici (ad esempio nel caso degli UUID). Impostare la formattazione di ogni cella come testo per risolvere il problema.
- Escludere gli eventi che non interessano l'utente da tutte le pagine in cui vengono visualizzati facendo clic sull'icona **Escludi eventi** ( ) (vedere Esclusione di eventi).
- Solo switch Flex. Risolvere i problemi che potrebbero verificarsi tra il certificato di sicurezza di XClarity Administrator e quello del modulo CMM nello chassis in cui è installato lo switch selezionando uno switch e facendo clic su **Tutte le azioni → Sicurezza → Risolvi certificati non attendibili** (vedere Risoluzione di un certificato server non attendibile).
- Aggiungere o rimuovere uno switch da un gruppo di risorse statico facendo clic su **Tutte le azioni → Gruppi → Aggiungi a gruppo** o **Tutte le azioni → Gruppi → Rimuovi da gruppo**.

Visualizzazione dei dettagli di uno switch

È possibile visualizzare informazioni dettagliate su uno switch gestito da Lenovo XClarity Administrator, inclusi i livelli di firmware e gli indirizzi IP.

Ulteriori informazioni:

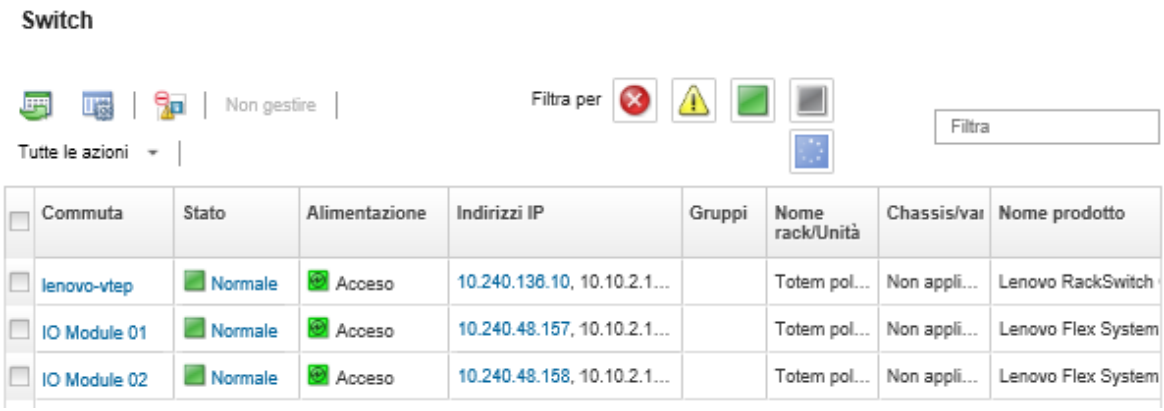
- XClarity Administrator: inventario
- XClarity Administrator: monitoraggio

Procedura

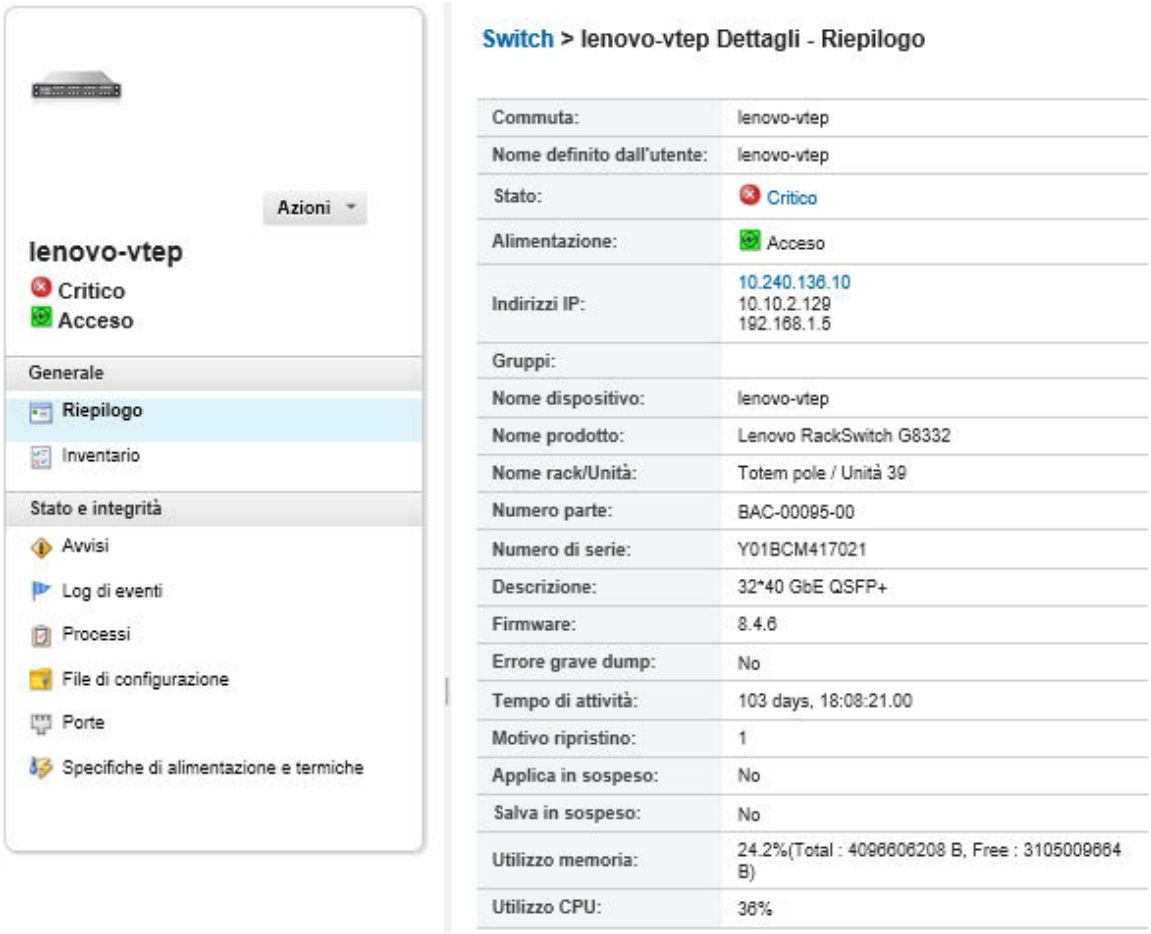
Per visualizzare i dettagli di uno specifico switch gestito da XClarity Administrator, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch con una vista tabulare di tutti gli switch installati nello chassis gestito.

È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. Inoltre, immettere del testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati.



Passo 2. Fare clic sullo switch nella colonna **Switch**. Verrà visualizzata la pagina di riepilogo che mostra le proprietà e un elenco dei componenti installati nello switch.



Passo 3. Completare una o più delle seguenti operazioni per visualizzare informazioni dettagliate sull'inventario:

Nota: Alcuni dettagli potrebbero non essere disponibili per tutti gli switch.

- Fare clic su **Riepilogo** per visualizzare un riepilogo dello switch, incluse le informazioni di sistema e il firmware (vedere Visualizzazione dello stato dei dispositivi di storage).
- Fare clic su **Dettagli inventario** per visualizzare i dettagli sui componenti dello switch, tra cui:
  - Livelli di firmware per lo switch
  - Dettagli della rete del controller di gestione, ad esempio il nome host, l'indirizzo IPv4, l'indirizzo IPv6 e gli indirizzi MAC
  - Dettagli delle risorse dello switch
- Fare clic su **Connettività I/O** per visualizzare dettagli di connettività per lo switch selezionato e le schede di rete associate installate al suo interno.
- Fare clic su **Avvisi** per visualizzare nel relativo elenco gli avvisi correlati allo switch (vedere Gestione degli avvisi).
- Fare clic su **Log eventi** per visualizzare nel relativo log gli eventi correlati allo switch (vedere Utilizzo degli eventi).
- Fare clic su **File di configurazione** per eseguire il backup e il ripristino della configurazione degli switch (vedere Backup e ripristino dei dati di configurazione di uno switch).
- Fare clic su **Cronologia distribuzione** per visualizzare le informazioni sui modelli di configurazione degli switch distribuiti (vedere Visualizzazione della cronologia di distribuzione delle configurazioni degli switch).
- Fare clic su **Processi** per visualizzare i file dei dati di configurazione di uno switch (vedere Monitoraggio dei processi).
- Fare clic su **Porte** per visualizzare lo stato e la configurazione di tutte le porte di uno switch gestito e per abilitare o disabilitare le porte dello switch.

  Nota: Per gli switch Flex, fare clic sull'icona **Aggiorna** () per raccogliere i dati correnti della porta. La raccolta dei dati potrebbe richiedere alcuni minuti.
- Fare clic su **light path** per visualizzare lo stato corrente di ciascun LED sullo switch.
- Fare clic su **Specifiche di alimentazione e termiche** per visualizzare informazioni su temperatura, alimentatori e ventole.

  Suggerimento: per raccogliere i dati relativi alle specifiche di alimentazione e termiche più recenti, utilizzare il pulsante di aggiornamento nel browser Web. La raccolta dei dati potrebbe richiedere alcuni minuti.

Al termine

Oltre a visualizzare il riepilogo e le informazioni dettagliate sullo switch, è possibile effettuare le seguenti operazioni:

- Visualizzare uno switch Flex nella vista grafica dello chassis o del rack facendo clic su **Azioni → Viste → Mostra nella vista rack** o **Azioni → Viste → Mostra nella vista chassis**.
- Visualizzare uno switch RackSwitch nella vista rack grafica facendo clic su **Azioni → Viste → Mostra nella vista rack**.
- Avviare l'interfaccia Web del controller di gestione per lo switch facendo clic sul collegamento **Indirizzo IP** (vedere Avvio dell'interfaccia del controller di gestione per uno switch).
- Avviare la console SSH dello switch (vedere Avvio di una sessione SSH remota per uno switch).
- Accendere e spegnere lo switch (vedere Accensione e spegnimento di uno switch).
- Solo switch RackSwitch. Modificare le informazioni di sistema selezionando uno switch e facendo clic su **Modifica proprietà**.

- Esportare le informazioni dettagliate sullo switch in un file CSV facendo clic su **Azioni → Inventario → Esporta inventario**.

  Nota:

  – Per ulteriori informazioni sui dati di inventario nel file CSV, vedere GET /switches/<*UUID_list*> API REST nella documentazione online di XClarity Administrator.

  – Durante l'importazione di un file CSV in Microsoft Excel, i valori di testo contenenti solo numeri vengono trattati come valori numerici (ad esempio nel caso degli UUID). Impostare la formattazione di ogni cella come testo per risolvere il problema.
- Escludere gli eventi che non interessano l'utente da tutte le pagine in cui vengono visualizzati facendo clic su **Azioni → Ripristino servizio → Eventi esclusi** (vedere Esclusione di eventi).
- Risolvere i problemi che potrebbero verificarsi tra il certificato di sicurezza di XClarity Administrator e quello di RackSwitch o del modulo CMM nello chassis in cui è installato lo switch Flex System, selezionando uno switch e facendo clic su **Azioni → Sicurezza → Risolvi certificati non attendibili** (vedere Risoluzione di un certificato server non attendibile).

Accensione e spegnimento di uno switch

È possibile accendere, spegnere e riavviare uno switch Flex System o RackSwitch da Lenovo XClarity Administrator.

Procedura

Per accendere o spegnere uno switch gestito, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch con una vista tabulare di tutti gli switch installati nello chassis gestito.

È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. Inoltre, immettere del testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati.

Passo 2. Selezionare lo switch da accendere, spegnere o riavviare.

Passo 3. Fare clic su **Tutte le azioni**, quindi selezionare una delle seguenti azioni di alimentazione:
- **Accendi** (solo switch Flex System)
- **Spegni** (solo switch Flex System)
- **Riavvia**. Lo switch viene riavviato una volta completate tutte le operazioni in esecuzione. Le operazioni avviate mentre lo switch viene riavviato vengono rifiutate.

Abilitare e disabilitare le porte di uno switch

È possibile abilitare e disabilitare le porte specifiche di uno switch RackSwitch o Flex System

Procedura

Per abilitare o disabilitare le porte di uno switch, completare le seguenti operazioni.

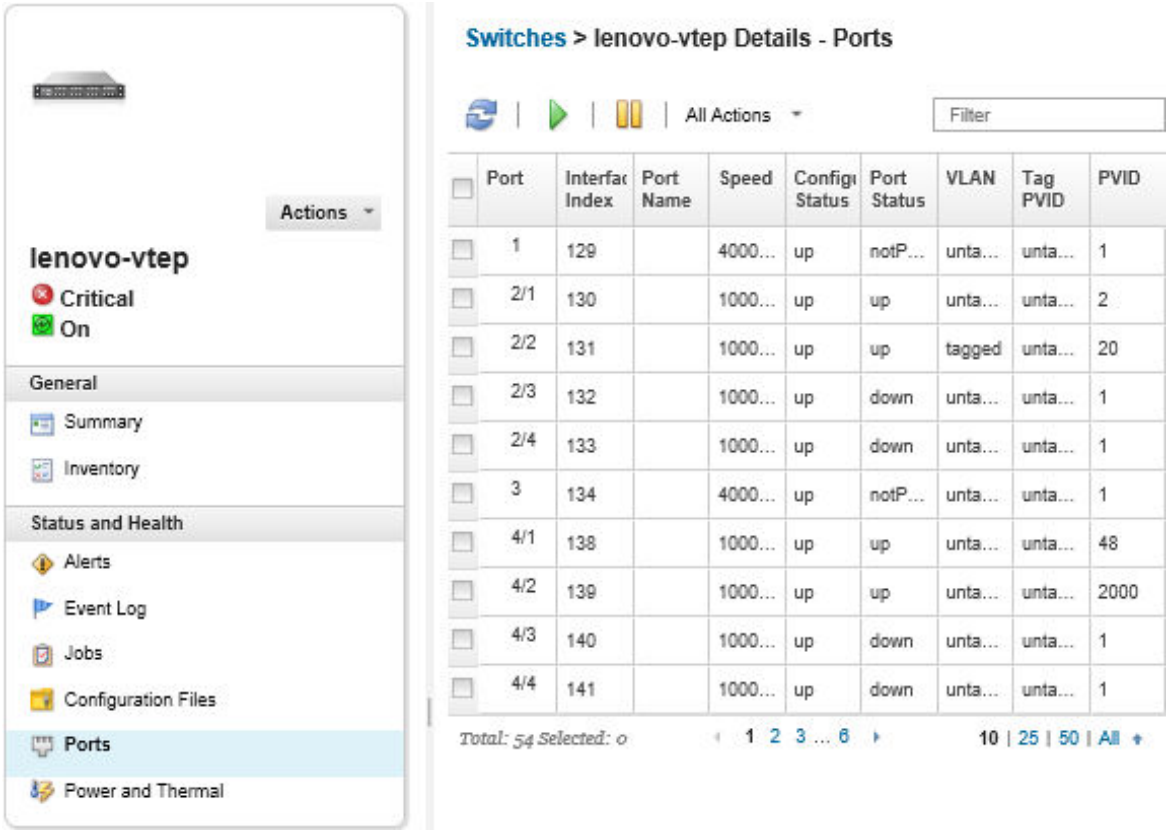
Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch con una vista tabulare di tutti gli switch installati nello chassis gestito.

È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. Inoltre, immettere del testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati.

Passo 2. Fare clic sullo switch nella colonna **Switch**. Verrà visualizzata la pagina di riepilogo che mostra le proprietà e un elenco dei componenti installati nello switch.

Passo 3. Fare clic su **Porte** nel riquadro di navigazione sinistro per visualizzare lo stato e la configurazione di tutte le porte dello switch:

Nota: Per gli switch Flex, fare clic sull'icona **Aggiorna** ( ) per raccogliere i dati correnti della porta. La raccolta dei dati potrebbe richiedere alcuni minuti



Passo 4. Selezionare la porta e fare clic sull'icona **Abilita** ( ) o **Disabilita** ( ).

Backup e ripristino dei dati di configurazione di uno switch

È possibile utilizzare Lenovo XClarity Administrator per eseguire il backup e il ripristino dei dati di configurazione degli switch RackSwitch e Flex System. È anche possibile esportare i file di configurazione di uno switch nel sistema locale e importare i file di configurazione di uno switch in XClarity Administrator.

Backup dei dati di configurazione di uno switch

È possibile eseguire il backup dei dati di configurazione per uno switch RackSwitch o Flex System. Quando si esegue il backup di uno switch, i dati di configurazione vengono importati in Lenovo XClarity Administrator dallo switch di destinazione come file di configurazione dello switch.

Procedura

Per eseguire il backup dei dati di configurazione per uno switch gestito, completare le seguenti operazioni.

- Per uno switch singolo:
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch con una vista tabulare di tutti gli switch installati nello chassis gestito.

     È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. Inoltre, immettere del testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati.

2. Fare clic sullo switch nella colonna **Switch**. Verrà visualizzata la pagina di riepilogo che mostra le proprietà e un elenco dei componenti installati nello switch.
3. Fare clic su **Configurazione** per visualizzare i file di configurazione per lo switch.
4. Fare clic sull'icona **Backup dei dati di configurazione** ( ) per eseguire il backup della configurazione dello switch.
5. (Facoltativo) Specificare un nome per il file di configurazione dello switch.

   Per i dispositivi CNOS, il nome del file può contenere caratteri alfanumerici e i seguenti caratteri speciali: carattere di sottolineatura (_), trattino (-) e punto (.). Per gli switch ENOS, il nome del file può contenere caratteri alfanumerici e qualsiasi carattere speciale.

   Se non viene specificato un nome del file, viene utilizzato il nome predefinito seguente: "<*switch_name*>_<*IP_address*>_<*timestamp*>.cfg."
6. (Facoltativo) Aggiungere un commento che descrive il backup.
7. Fare clic su **Backup** per eseguire subito il backup dei di configurazione dello switch oppure fare clic su **Pianifica** per pianificare l'esecuzione di questo backup in un secondo momento.

   Se si sceglie di pianificare un backup, è possibile selezionare **Sovrascrivi** per eseguire il backup dei dati di configurazione dello switch nello stesso file per ogni processo eseguito, sovrascrivendo il contenuto. Se si sceglie di non sovrascrivere il file, i nomi dei file dei successivi backup vengono aggiunti con un numero univoco (ad esempio, MyBackup_33.cfg).

   Nota: Quando si pianifica un backup, è possibile scegliere nomi di file dinamici o commenti per ogni processo pianificato.

- Per più switch:
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch con una vista tabulare di tutti gli switch installati nello chassis gestito.
  2. Selezionare uno o più switch.
  3. Fare clic su **Tutte le azioni → Configurazione → Esegui backup del file di configurazione**.
  4. (Facoltativo) Specificare un nome per il file di configurazione dello switch.

     Per i dispositivi CNOS, il nome del file può contenere caratteri alfanumerici e i seguenti caratteri speciali: carattere di sottolineatura (_), trattino (-) e punto (.). Per gli switch ENOS, il nome del file può contenere caratteri alfanumerici e qualsiasi carattere speciale.

     Se non viene specificato un nome del file, viene utilizzato il nome predefinito seguente: "<*switch_name*>_<*IP_address*>_<*timestamp*>.cfg."
  5. (Facoltativo) Aggiungere un commento che descrive il backup.

6. Fare clic su **Backup** per eseguire subito il backup dei di configurazione dello switch oppure fare clic su **Pianifica** per pianificare l'esecuzione di questo backup in un secondo momento.

   Se si sceglie di pianificare un backup, è possibile selezionare **Sovrascrivi** per eseguire il backup dei dati di configurazione dello switch nello stesso file per ogni processo eseguito, sovrascrivendo il contenuto. Se si sceglie di non sovrascrivere il file, i nomi dei file dei successivi backup vengono aggiunti con un numero univoco (ad esempio, MyBackup_33.cfg).

   Nota: Quando si pianifica un backup, è possibile scegliere nomi di file dinamici o commenti per ogni processo pianificato.

Al termine

Una volta completato il processo di backup, il file di configurazione dello switch viene aggiunto alla scheda **File di configurazione** nella pagina dei dettagli dello switch.

Da questa pagina, è possibile eseguire le seguenti azioni su un file di configurazione dello switch selezionato:

- Ripristinare la configurazione dello switch selezionando il file di configurazione dello switch e facendo clic sull'icona **Ripristina dati di configurazione** ( ).
- Eliminare i file di configurazione dello switch da XClarity Administrator facendo clic sull'icona **Elimina** ( ).
- Esportare i file di configurazione dello switch nel sistema locale selezionando i file e facendo clic sull'icona **Esporta file di configurazione** ( ).
- Importare i file di configurazione dello switch in XClarity Administrator facendo clic sull'icona **Importa file di configurazione** ( ).

Ripristino dei dati di configurazione di uno switch

È possibile ripristinare i dati di configurazione di cui è stato eseguito il backup o che sono stati importati in Lenovo XClarity Administrator per uno switch Flex System o RackSwitch. Il file dei dati di configurazione di uno switch viene scaricato da XClarity Administrator sullo switch di destinazione e la configurazione viene applicata automaticamente.

I file di configurazione sono associati a uno specifico switch. È possibile ripristinare un file di configurazione solo sullo switch a cui è associato. Non è possibile utilizzare un file di configurazione di cui è stato eseguito il backup di uno switch per ripristinare la configurazione di un altro switch.

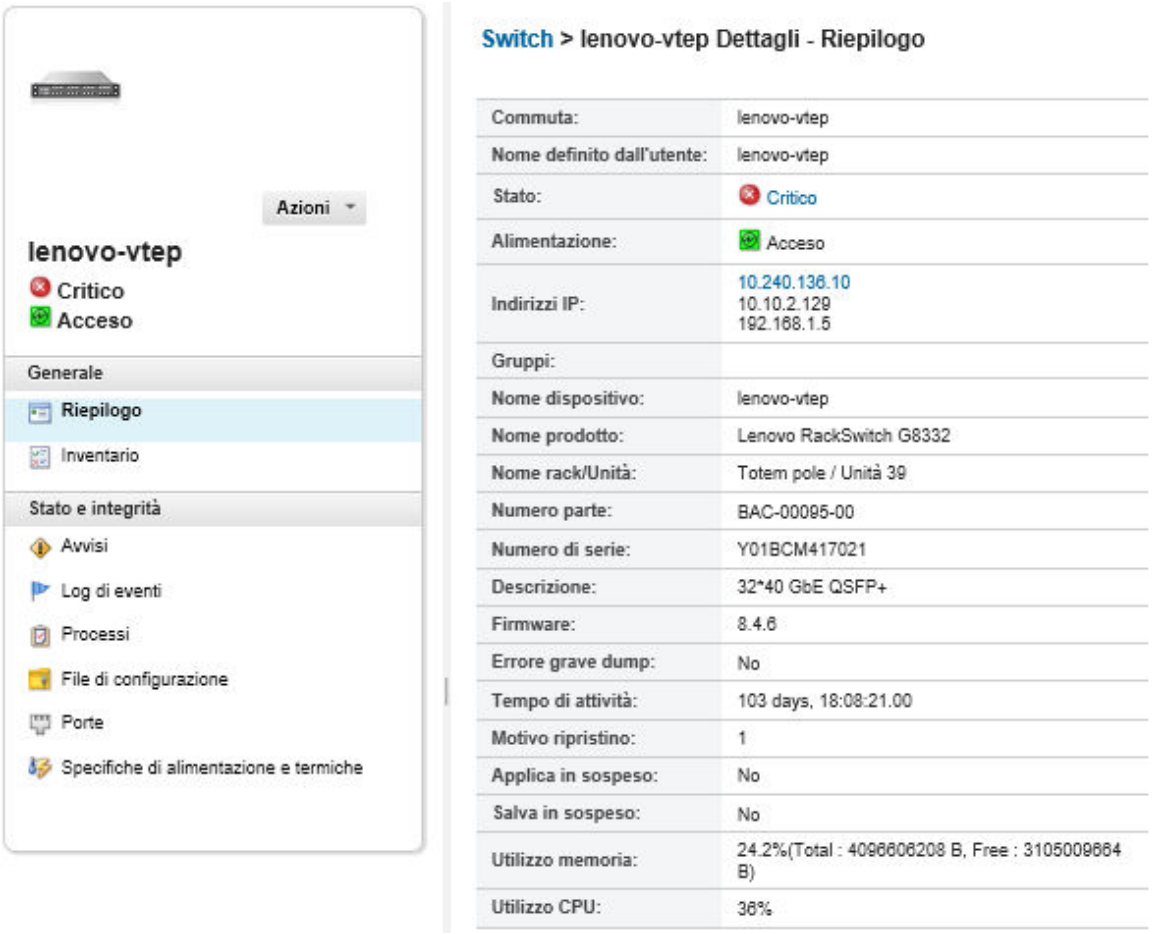
Procedura

Per ripristinare i dati di configurazione su uno switch gestito, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch con una vista tabulare di tutti gli switch installati nello chassis gestito.

   È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. Inoltre, immettere del testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati.

Passo 2. Fare clic sullo switch nella colonna **Switch**. Verrà visualizzata la pagina di riepilogo che mostra le proprietà e un elenco dei componenti installati nello switch.



Passo 3. Fare clic su **File di configurazione** per visualizzare i file di configurazione per lo switch.

Passo 4. Selezionare il file di configurazione che si desidera ripristinare sullo switch e fare clic sull'icona **Ripristina dati di configurazione** ( ). Viene visualizzata la finestra di dialogo "Ripristina".

Passo 5. (Solo switch che eseguono CNOS) Scegliere se riavviare lo switch al termine dell'operazione di ripristino.

Se si sceglie di non riavviare lo switch automaticamente è necessario riavviare manualmente lo switch CNOS per attivare i dati della configurazione ripristinata. Se il processo richiede troppo

tempo e si verifica un'operazione di salvataggio (ad esempio, se una porta è abilitata o disabilitata), l'operazione di ripristino viene interrotta e vengono utilizzati i dati della configurazione in esecuzione.

Passo 6. Fare clic su **Ripristina** per ripristinare subito i dati di configurazione dello switch oppure fare clic su **Pianifica** per pianificare l'esecuzione di questo processo di ripristino in un secondo momento.

Nota: Prestare attenzione quando si pianificano processi di ripristino periodici. Se lo switch viene reimpostato a una configurazione precedente, consultare la Processi pianificati per i processi di ripristino pianificati.

Esportazione e importazione dei file di configurazione di uno switch

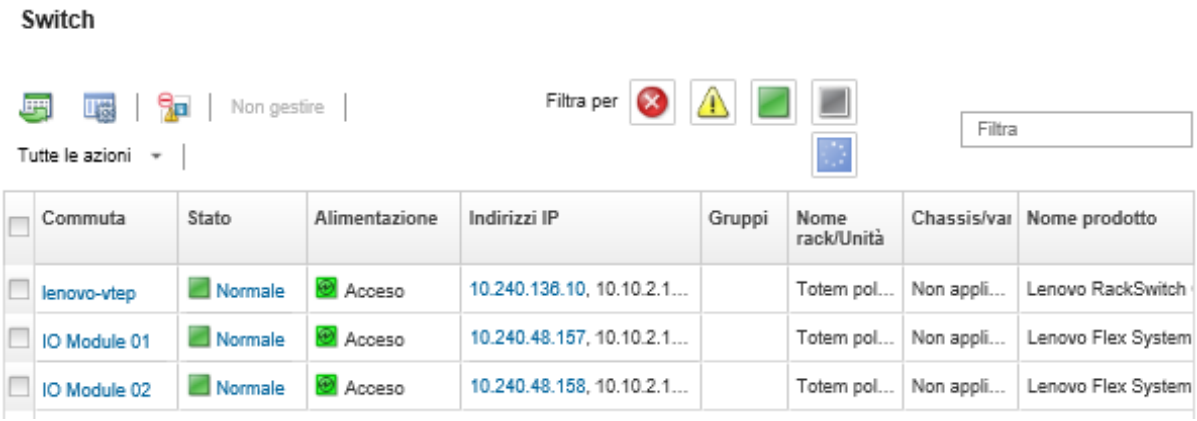
È possibile esportare i file di configurazione di uno switch nel sistema locale e importare i file di configurazione di uno in Lenovo XClarity Administrator.

Procedura

Per eseguire il backup dei dati di configurazione per uno switch gestito, completare le seguenti operazioni.

- Esportare i file di configurazione di uno switch
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch con una vista tabulare di tutti gli switch installati nello chassis gestito.

     È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. Inoltre, immettere del testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati.



  2. Fare clic sullo switch nella colonna **Switch**. Verrà visualizzata la pagina di riepilogo che mostra le proprietà e un elenco dei componenti installati nello switch.
  3. Fare clic su **Configurazione** per visualizzare i file di configurazione per lo switch.
  4. Selezionare il file di configurazione dello switch da importare.
  5. Fare clic sull'icona **Esporta file di configurazione** ( ) per eseguire il backup della configurazione dello switch.
- Importare i file di configurazione di uno switch
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch con una vista tabulare di tutti gli switch installati nello chassis gestito.

     È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. Inoltre, immettere del testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati.

2. Fare clic sullo switch nella colonna **Switch**. Verrà visualizzata la pagina di riepilogo che mostra le proprietà e un elenco dei componenti installati nello switch.
3. Fare clic su **Configurazione** per visualizzare i file di configurazione per lo switch.
4. Fare clic sull'icona **Importa file di configurazione** ( ) per eseguire il backup della configurazione dello switch.
5. Immettere il nome del file di configurazione dello switch oppure fare clic su **Sfoglia** per individuare il file di avvio che si desidera importare.
6. **Facoltativo:** immettere una descrizione per il file di configurazione dello switch.
7. Fare clic su **Importa**.

   Se si chiude la scheda o la finestra del browser Web in cui il file viene caricato prima del completamento dell'operazione, l'importazione non riesce.

Avvio dell'interfaccia del controller di gestione per uno switch

È possibile avviare l'interfaccia Web del controller di gestione per uno switch RackSwitch o Flex System che esegue ENOS da Lenovo XClarity Administrator.

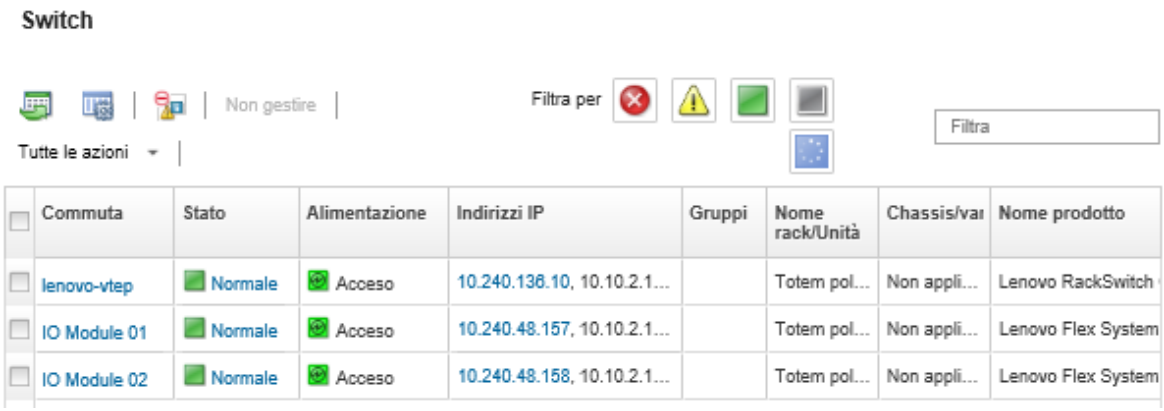
Procedura

Per avviare l'interfaccia del controller di gestione per uno switch, attenersi alla procedura descritta di seguito.

Nota: Non è supportato l'avvio di un'interfaccia Web del controller di gestione da XClarity Administrator mediante il browser Web Safari.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch con una vista tabulare di tutti gli switch installati nello chassis gestito.

È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. Inoltre, immettere del testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati.



Passo 2. Selezionare lo switch e fare clic su **Tutte le azioni → Avvia → Interfaccia Web di gestione**. Verrà visualizzata l'interfaccia Web del controller di gestione per lo switch.

Suggerimento: è inoltre possibile avviare l'interfaccia del controller di gestione facendo clic sul collegamento dell'indirizzo IP nella colonna **Indirizzo IP** e nelle pagine di riepilogo e dei dettagli dello switch.

Passo 3. Eseguire il login all'interfaccia del controller di gestione.

Suggerimento: per gli switch Flex, utilizzare le credenziali utente XClarity Administrator. Per gli switch XClarity Administrator, utilizzare le credenziali switch.

Avvio di una sessione SSH remota per uno switch

È possibile avviare una sessione SSH remota per uno switch RackSwitch o Flex gestito da Lenovo XClarity Administrator. Dalla sessione SSH remota è possibile utilizzare l'interfaccia della riga di comando per eseguire le attività di gestione non fornite da XClarity Administrator.

Prima di iniziare

Verificare che lo switch sia configurato per abilitare il protocollo SSH. Per gli switch RackSwitch, il protocollo SSH è abilitato quando lo switch è gestito da XClarity Administrator. Per gli switch Flex, il protocollo SSH è in genere abilitato per impostazione predefinita. In caso contrario, dovrà essere abilitato prima che lo switch venga gestito da XClarity Administrator.

Procedura

Per avviare una sessione SSH remota per uno switch gestito, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch con una vista tabulare di tutti gli switch installati nello chassis gestito.

È possibile ordinare le colonne della tabella per individuare più facilmente gli switch che si desidera gestire. Inoltre, immettere del testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati.

Passo 2. Selezionare lo switch per avviare una sessione SSH.

Passo 3. Fare clic su **Tutte le azioni → Avvia → Console SSH**.

Passo 4. Se necessario, eseguire il login allo switch utilizzando l'ID utente e la password personali.

Modifica delle proprietà di sistema per uno switch

È possibile modificare le proprietà di sistema per uno specifico switch Flex System o RackSwitch.

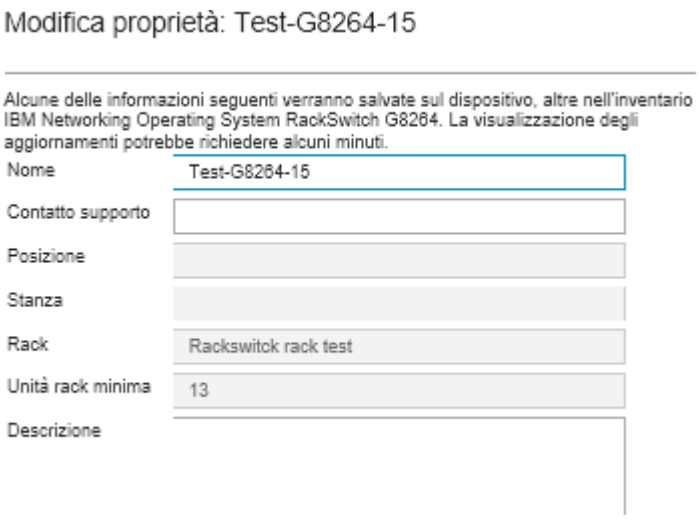
Procedura

Per modificare le proprietà di sistema, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Hardware → Switch** per visualizzare la pagina Switch.

Passo 2. Selezionare lo switch da aggiornare.

Passo 3. Fare clic su **Tutte le azioni → Inventario → Modifica proprietà** per visualizzare la finestra di dialogo Modifica.



Passo 4. Modificare le seguenti informazioni, in base alle esigenze.

- Nome dello switch
- Contatto supporto
- Descrizione

Nota: Posizione, ambiente, rack e proprietà dell'unità inferiore del rack vengono aggiornati da XClarity Administrator quando si aggiungono o rimuovono dispositivi da un rack nell'interfaccia Web (vedere Gestione dei rack).

Passo 5. Fare clic su **Salva**.

Nota: Quando vengono modificate queste proprietà, è possibile che si verifichi un breve ritardo nella visualizzazione delle modifiche nell'interfaccia Web di XClarity Administrator.

Risoluzione di credenziali memorizzate scadute o non valide per uno switch

Quando una credenziale memorizzata scade o non è più utilizzabili su un dispositivo, lo stato del dispositivo viene visualizzato come "Offline."

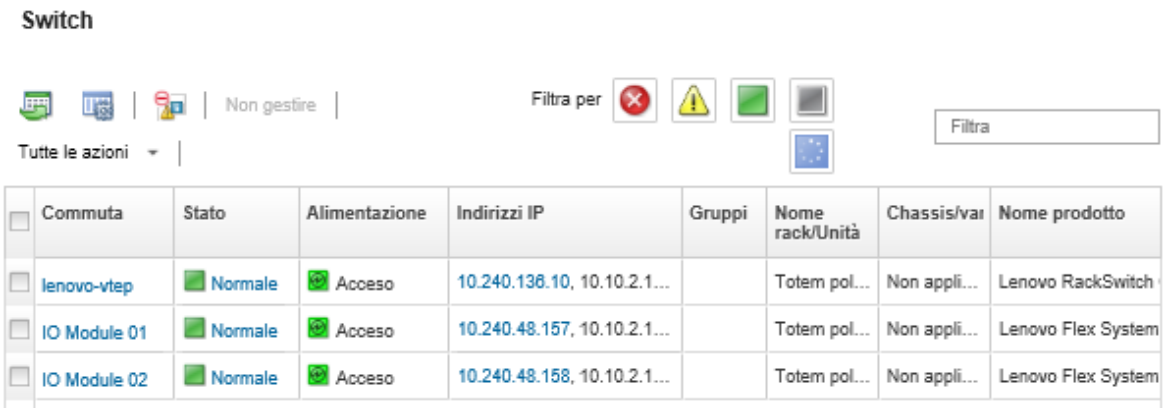
Procedura

Per risolvere le credenziali memorizzate scadute o non valide per uno switch, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware → Switch**. Verrà visualizzata la pagina Switch contenente una vista tabulare di tutti gli switch gestiti.

Passo 2. Fare clic sull'intestazione di colonna **Alimentazione** per raggruppare tutti gli switch offline nella parte superiore della tabella.

È possibile ordinare le colonne della tabella per individuare più facilmente lo switch che si desidera gestire. Inoltre, è possibile immettere il testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** per filtrare ulteriormente gli switch visualizzati.



Passo 3. Selezionare lo switch da risolvere.

Passo 4. Fare clic su **Tutte le azioni → Sicurezza → Modifica credenziali memorizzate**.

Passo 5. Modificare la password per la credenziale memorizzata o selezionare un'altra credenziale memorizzata da utilizzare per il dispositivo gestito.

Nota: Se è stato gestito più di un dispositivo utilizzando le stesse credenziali memorizzate ed è stata modificata la password per le credenziali memorizzate, la modifica della password interessa tutti i dispositivi che attualmente utilizzano le credenziali memorizzate.

Ripristino della gestione con uno switch dopo un errore del server di gestione

È possibile ripristinare la gestione di uno switch che non è stata annullata correttamente (ad esempio, a causa di problemi di connettività durante l'annullamento della gestione o di un errore di Lenovo XClarity Administrator di gestione).

Procedura

- Gestire nuovamente lo switch utilizzando l'opzione **Forza gestione** (vedere Gestione degli switch).
- Per rimuovere definitivamente una configurazione specifica di XClarity Administrator in uno switch la cui gestione non è stata annullata correttamente e che non verrà più gestito, attenersi alla procedura descritta di seguito.
  - Gestire nuovamente lo switch utilizzando l'opzione **Forza gestione** (vedere Gestione degli switch), quindi annullarne la gestione per rimuovere la configurazione (vedere Annullamento della gestione di uno switch).
  - (ENOS) Eseguire il login allo switch utilizzando la relativa porta di console oppure una sessione SSH o telnet ed eseguire i seguenti comandi di configurazione nell'ordine specificato per cancellare la configurazione dello switch.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Annullamento della gestione di uno switch

È possibile rimuovere uno switch dalla gestione da parte di Lenovo XClarity Administrator. Questo processo è detto *annullamento della gestione.*

Prima di iniziare

È possibile abilitare XClarity Administrator per annullare automaticamente la gestione dei dispositivi che restano offline per un periodo di tempo specifico. Questa opzione è disabilitata per impostazione predefinita. Per abilitare l'annullamento della gestione automatica dei dispositivi offline, fare clic su **Hardware → Rileva e gestisci nuovi dispositivi** dal menu di XClarity Administrator, quindi fare clic su **Modifica** accanto a **Annulla gestione dispositivi offline è Disabilitato**. Quindi, selezionare **Abilita annullamento gestione dispositivi offline** e impostare l'intervallo di tempo. Per impostazione predefinita, i dispositivi non vengono gestiti dopo essere rimasti offline per 24 ore.

Prima di annullare la gestione di uno switch, accertarsi che nello switch non siano in esecuzione processi attivi.

Informazioni su questa attività

Quando si annulla la gestione di uno switch, XClarity Administrator conserva alcune informazioni sullo switch. Queste informazioni verranno riapplicate quando lo stesso switch verrà nuovamente gestito.

Suggerimento: tutti i dispositivi dimostrativi aggiunti facoltativamente durante la configurazione iniziale sono nodi di uno chassis. Per annullare la gestione dei dispositivi dimostrativi, annullare la gestione dello chassis mediante l'opzione **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.

Procedura

Per annullare la gestione di uno switch, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator fare clic su **Hardware → Switch** per visualizzare la pagina Switch.

Passo 2. Selezionare uno o più switch dagli elenchi degli switch gestiti.

Passo 3. Fare clic su **Annulla gestione switch**. Viene visualizzata la finestra di dialogo Non gestire.

Passo 4. **Facoltativo:** selezionare **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.

Importante: quando si annulla la gestione di hardware dimostrativo, verificare di aver selezionato questa opzione.

Passo 5. Fare clic su **Non gestire**.La finestra di dialogo Non gestire mostra l'avanzamento di ogni operazione nel processo di annullamento della gestione.

Passo 6. Al termine del processo di annullamento della gestione, fare clic su **OK**.

Ripristino di uno switch la cui gestione non è stata annullata correttamente

Se uno switch è gestito da Lenovo XClarity Administrator e si verificano errori in XClarity Administrator, è possibile ripristinare le funzioni di gestione finché il server di gestione non verrà ripristinato o sostituito.

Procedura

- Gestire nuovamente lo switch utilizzando l'opzione **Forza gestione** (vedere Gestione degli switch).
- Per rimuovere definitivamente una configurazione specifica di XClarity Administrator in uno switch la cui gestione non è stata annullata correttamente e che non verrà più gestito, attenersi alla procedura descritta di seguito.
  - Gestire nuovamente lo switch utilizzando l'opzione **Forza gestione** (vedere Gestione degli switch), quindi annullarne la gestione per rimuovere la configurazione (vedere Annullamento della gestione di uno switch).
  - (ENOS) Eseguire il login allo switch utilizzando la relativa porta di console oppure una sessione SSH o telnet ed eseguire i seguenti comandi di configurazione nell'ordine specificato per cancellare la configurazione dello switch.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Capitolo 11. Configurazione dei server mediante i pattern di configurazione

I pattern server vengono utilizzati per eseguire rapidamente il provisioning o il preprovisioning (server rack e tower e nodi di elaborazione) da un singolo set di impostazioni di configurazione definite.

Ulteriori informazioni:

- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: pattern di configurazione

Prima di iniziare

Al termine del periodo di prova di 90 giorni, è possibile continuare a utilizzare XClarity Administrator per gestire e monitorare l'hardware gratuitamente; tuttavia, è necessario acquistare le licenze per l'attivazione di tutte le funzioni per ciascun server gestito che supporta le funzioni avanzate di XClarity Administrator per continuare a utilizzare la funzione di configurazione del server. Lenovo XClarity Pro dà diritto a usufruire del servizio di assistenza e supporto e a utilizzare la licenza per l'attivazione di tutte le funzioni. Per ulteriori informazioni sull'acquisto di Lenovo XClarity Pro, contattare un rappresentante Lenovo o un business partner autorizzato. Per ulteriori informazioni, vedere Installazione della licenza di abilitazione di tutte le funzionalità nella documentazione online di XClarity Administrator.

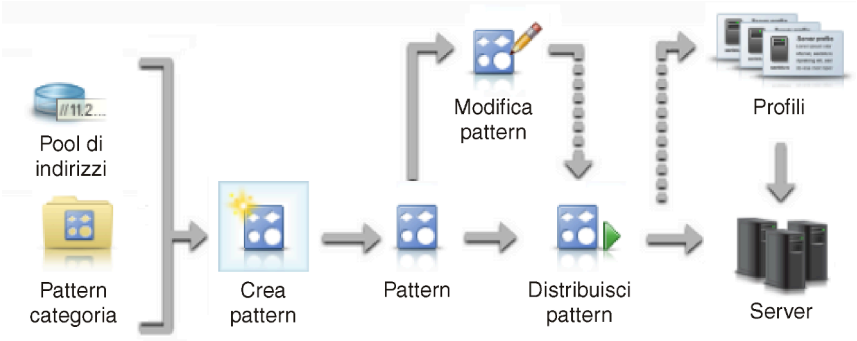
Consultare Considerazioni sulla configurazione per importanti informazioni sul supporto alla configurazione per specifici server e dispositivi.

Informazioni su questa attività

È possibile utilizzare pattern server in XClarity Administrator per configurare storage locale, adattatori I/O, ordine di avvio e altre impostazioni del controller di gestione della scheda di base e UEFI (Unified Extensible Firmware Interface) nei server gestiti. I pattern server integrano inoltre il supporto per la virtualizzazione degli indirizzi I/O, pertanto è possibile virtualizzare le connessioni fabric del server oppure reimpiegare i server senza interruzione nel fabric. È inoltre possibile avviare richieste di modifica di suddivisione in zone SAN prima di ricevere nuovo hardware virtualizzando (preconfigurando) indirizzi Fibre Channel.

Procedura

La seguente figura mostra il flusso di lavoro per la configurazione di server gestiti. Le frecce piene indicano le azioni intraprese dall'utente. Le frecce tratteggiate indicano le azioni eseguite automaticamente da XClarity Administrator.



Passo 1. **Creare pool di indirizzi.**Un *pool di indirizzi* è un set definito di intervalli di indirizzi. Lenovo XClarity Administrator utilizza pool di indirizzi per assegnare indirizzi IP e I/O a singoli server quando vengono distribuiti i pattern server.

Per ulteriori informazioni sulla creazione di pool di indirizzi, vedere Definizione di pool di indirizzi.

Passo 2. **Creare pattern categoria.**

Un *pattern categoria* raggruppa le impostazioni firmware correlate per consentirne il riutilizzo in più pattern server. È possibile creare pattern per le seguenti categorie di firmware:

- Informazioni di sistema
- Interfacce di gestione
- Dispositivi e porte I/O
- Destinazioni di avvio FC
- Porte di adattatori I/O

Per ulteriori informazioni sulla creazione di pattern categoria, vedere Utilizzo di pattern server.

Passo 3. **Creare un pattern server.**

Un *pattern server* rappresenta le configurazioni server precedenti all'installazione del sistema operativo, che includono la configurazione dello storage locale e degli adattatori I/O, le impostazioni di avvio e altre impostazioni firmware del controller di gestione della scheda di base e UEFI (Unified Extensible Firmware Interface). Un pattern server viene utilizzato come pattern globale per configurare rapidamente più server alla volta.

È possibile definire più pattern server per rappresentare configurazioni diverse utilizzate nel centro dati.

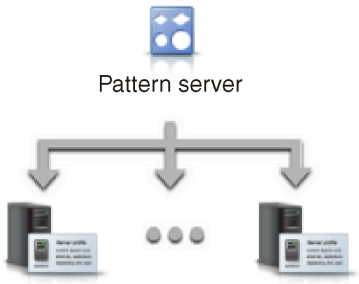
Quando si definisce un pattern server, selezionare i pattern categoria e i pool di indirizzi necessari per progettare la configurazione desiderata per un gruppo specifico di server. Un pattern categoria raggruppa le impostazioni di configurazione correlate per consentirne il riutilizzo in più pattern server.

È possibile creare un pattern server da zero per server Converged, Flex System, NeXtScale e System x al fine di definire la configurazione desiderata prima di ricevere l'hardware. In alternativa, è possibile creare un pattern server da un server gestito esistente. Se si crea un pattern server da un server esistente, XClarity Administrator apprende i pattern categoria dal server selezionato.

Per ulteriori informazioni sulla creazione di pattern server, vedere Creazione di un pattern server.

Passo 4. **Distribuire il pattern server.**

È possibile distribuire un pattern server a uno o più server singolarmente, oppure a gruppi di server. È ad esempio possibile distribuire un pattern server in uno chassis in modo che tutti i nodi di elaborazione al suo interno vengano configurati in modo identico. Durante la distribuzione, XClarity Administrator crea un profilo per ciascun server in cui è stato distribuito il pattern server. Ogni *profilo del server* rappresenta la configurazione specifica per un singolo server. Eredita le impostazioni dal pattern server e contiene inoltre informazioni specifiche del server (tra cui gli indirizzi IP e MAC assegnati). Poiché il profilo del server eredita le impostazioni dal pattern server, la modifica di quest'ultimo viene automaticamente riflessa nel profilo. In questo modo è possibile gestire configurazioni comuni in un'unica posizione.



Nota: Le impostazioni di un server possono diventare non conformi al profilo del server, se le impostazioni vengono modificate senza utilizzare i pattern di configurazione o se si è verificato un problema durante la distribuzione, come un problema relativo a un firmware o a un'impostazione non valida. È possibile determinare lo stato della conformità di ciascun server dalla pagina "Pattern di configurazione: Profili server".

È possibile distribuire un pattern server in:

- **Server esistenti**. Viene creato un profilo del server per ciascun server. Il profilo viene attivato in seguito al riavvio del server associato.
- **Vani vuoti in uno chassis esistente**. Viene creato un profilo del server per ciascun vano vuoto. Il profilo del server associato al vano vuoto potrà quindi essere attivato in seguito all'installazione fisica del nodo di elaborazione.
- **Segnaposto per uno chassis non ancora ricevuto**. È possibile eseguire il preprovisioning dei nodi di elaborazione in uno chassis non ancora ricevuto definendo uno *chassis segnaposto* da utilizzare come destinazione del pattern server prima di ricevere l'hardware. Lo chassis segnaposto aggrega tutti i profili del server creati per ciascun vano vuoto dei nodi di elaborazione. Una volta ricevuto l'hardware, sarà quindi possibile assegnare i profili del server a tutti i nodi di elaborazione nel nuovo chassis distribuendo lo chassis segnaposto nel nuovo chassis. Ciascun profilo viene attivato in seguito al riavvio del nodo di elaborazione associato.

Nota: È possibile distribuire un pattern server in più server, ma non è possibile distribuire più pattern in un singolo server.

Per ulteriori informazioni sulla distribuzione di un pattern server, vedere Distribuzione di un pattern server in un server e Distribuzione di uno chassis segnaposto.

Passo 5. **Modificare il pattern server.**

I pattern server consentono di controllare una configurazione comune da un'unica posizione. Le impostazioni non vengono più aggiornate direttamente nei server: l'utente aggiorna i pattern categoria e server e le modifiche vengono automaticamente distribuite in tutti i profili associati e nei relativi server.

Per ulteriori informazioni sulla modifica di un pattern server, vedere Modifica di un pattern server.

Considerazioni sulla configurazione

Prima di iniziare la configurazione dei server con Lenovo XClarity Administrator, esaminare le seguenti considerazioni importanti.

- Se un profilo del server include livelli di firmware precedenti e si aggiorna il firmware ai livelli successivi, XClarity Administrator confronta le impostazioni del profilo memorizzate con le impostazioni del server e segnala "Non conforme". Passare il cursore sullo stato "Non conforme" per determinare il motivo della non conformità.

È possibile modificare manualmente lo stato dei dispositivi non conformi in "Conforme" senza ridistribuire il profilo selezionando i dispositivi e facendo quindi clic su **Tutte le azioni → Rendi conforme**.

- Dopo l'aggiornamento del firmware (come UEFI, BMC o i controller I/O) su un server, alcune configurazioni potrebbero cambiare (ad esempio, quando si aggiungono nuovi elementi, si eliminano elementi esistenti oppure si modificano i comportamenti o l'intervallo di valori di un elemento). Di conseguenza, il profilo del server potrebbe diventare non conforme oppure l'applicazione del pattern server potrebbe avere esito negativo se il pattern viene creato utilizzando un livello di firmware precedente. In questo caso, si consiglia di scegliere di apprendere un nuovo pattern basato sul firmware aggiornato o di modificare il pattern non riuscito per escludere la configurazione di elementi specifici e quindi applicare tale pattern al server.
- L'adattatore QLogic 8200 2-Port 10GbE SFP+ VFA non dispone di valori validi per queste impostazioni: iSCSIFirstTargetParameters_iSCSIName, iSCSISecondTargetParameters_iSCSIName e IPv6LinkLocalAddress. È necessario correggere manualmente questi valori nella configurazione del sistema prima di conoscere il pattern di configurazione del server o di correggere i valori nel pattern di configurazione acquisito.
- Per i nodi di elaborazione Flex System x240 e x440 con adattatori RAID integrati, i pattern server che definiscono le definizioni della configurazione RAID possono essere distribuiti solo a uno o più server che non dispongono di configurazioni RAID esistenti. Se un pattern server viene distribuito a un server che dispone di una configurazione RAID esistente, gli array e i volumi esistenti non verranno sovrascritti. Per applicare la configurazione RAID definita nel pattern server, è necessario innanzitutto cancellare la configurazione RAID esistente dei server (vedere Reimpostazione dei valori predefiniti degli adattatori di storage) e quindi ridistribuire il profilo del server selezionando il server e facendo clic su **Altro → Distribuisci profilo server**.
- I controller di storage integrati nei server Flex System x220, Flex System x222 e ThinkSystem supportano configurazioni RAID basate su software. Tuttavia, la configurazione di RAID software mediante i pattern di configurazione non è supportata.
- Quando si configurano le impostazioni RAID utilizzando Pattern di configurazione, se il server è spento, il server viene avviato automaticamente con la configurazione BIOS/UEFI, prima di attivare il profilo del server.
- Per i server ThinkServer, Pattern di configurazione non è supportato.
- Determinati dispositivi I/O non possono essere configurati utilizzando i pattern server. Per ulteriori informazioni, vedere Supporto XClarity Administrator - Pagina Web sulla compatibilità.
- Se le funzioni avanzate (come SPAR, Easy Connect e stack) sono abilitate sugli switch Flex EN4093R, CN4093, SI4093 o SI4091, le configurazioni di rete potrebbero non essere applicate correttamente sulle porte interne.
- Per impostazione predefinita, lo switch Flex SI4093 viene fornito con la funzione SPAR abilitata. Se si desidera distribuire le impostazioni di rete utilizzando i pattern porta per le porte interne di questi switch, è necessario rimuovere manualmente le porte interne dello switch dalla funzione SPAR oppure rimuovere le configurazioni SPAR dallo switch.
- Si consiglia di *non* utilizzare XClarity Administrator per configurare le appliance Converged e ThinkAgile utilizzando i pattern di configurazione.
- Verificare che tutte le porte disponibili siano abilitate sugli adattatori installati prima di creare pattern di configurazione da un server esistente, in modo che tutte le impostazioni e le porte disponibili siano incluse nel pattern. Quindi, se necessario, è possibile disabilitare tutte le porte utilizzando le impostazioni appropriate definite nel pattern. Se le porte sono disabilitate quando viene creato il pattern, potrebbe non essere possibile crearlo e distribuirlo correttamente.

Definizione di pool di indirizzi

Un *pool di indirizzi* è un set definito di intervalli di indirizzi. Lenovo XClarity Administrator utilizza pool di indirizzi per assegnare indirizzi IP e I/O a singoli server quando vengono distribuiti i pattern server.

Informazioni su questa attività

XClarity Administrator supporta pool di indirizzi IP e I/O.

pool di indirizzi IP

I *pool di indirizzi IP* definiscono intervalli di indirizzi IP per l'utilizzo durante la configurazione dell'interfaccia di rete del controller di gestione della scheda di base dei server. È possibile utilizzare o personalizzare pool di indirizzi predefiniti oppure è possibile crearne nuovi in base alle esigenze. Durante la creazione di pattern server, è possibile scegliere il pool di indirizzi IP da utilizzare in fase di distribuzione. Una volta distribuito il pattern server, gli indirizzi IP verranno allocati dal pool selezionato e assegnati a singoli controller di gestione.

Nota: Se la configurazione di rete dei controller di gestione è soddisfacente, non utilizzare questa opzione.

Attenzione:

- Accertarsi di selezionare un intervallo secondario di indirizzi IP che non entri in conflitto con gli indirizzi I/O esistenti nel centro dati.
- Verificare che gli indirizzi IP negli intervalli specificati appartengano alla stessa sottorete e siano raggiungibili da XClarity Administrator.
- Accertarsi che gli indirizzi IP negli intervalli specificati siano univoci per ciascun dominio XClarity Administrator e per gli strumenti di gestione IP esistenti al fine di evitare conflitti negli indirizzi.

L'intervallo globale del pool di indirizzi viene ricavato dalla lunghezza del prefisso di instradamento specificata e dal gateway o dall'intervallo iniziale. È possibile creare pool di dimensioni diverse in base alla lunghezza del prefisso di instradamento specificata, ma gli intervalli globali dei pool devono essere univoci all'interno del dominio XClarity Administrator. Gli intervalli vengono quindi creati dall'intervallo globale del pool.

Gli intervalli di indirizzi possono essere utilizzati per separare gli host (ad esempio, per tipo di sistema operativo, carico di lavoro e attività). Gli intervalli possono inoltre essere associati a regole di rete aziendali.

Pool di indirizzi Ethernet

I *pool di indirizzi Ethernet* sono raccolte di indirizzi MAC univoci che possono essere assegnati alle schede di rete durante la configurazione di server. È possibile utilizzare o personalizzare pool di indirizzi predefiniti oppure è possibile crearne nuovi in base alle esigenze. Durante la creazione di pattern server, è possibile scegliere il pool di indirizzi Ethernet da utilizzare in fase di distribuzione. Una volta distribuito il pattern server, gli indirizzi verranno allocati dal pool selezionato e assegnati a singole porte di adattatori.

È disponibile il seguente pool predefinito di indirizzi MAC:
- Pool di indirizzi MAC Lenovo

Per un elenco degli intervalli di indirizzi MAC in questo pool, vedere Pool di indirizzi Ethernet (MAC).

Pool di indirizzi Fibre Channel

I *pool di indirizzi Fibre Channel* sono raccolte di indirizzi WWNN e WWPN univoci che possono essere assegnati agli adattatori Fibre Channel durante la configurazione di server. È possibile utilizzare o personalizzare pool di indirizzi predefiniti oppure è possibile crearne nuovi in base alle esigenze. Durante la creazione di pattern server, è possibile scegliere il pool di indirizzi Fibre Channel da utilizzare in fase di distribuzione. Una volta distribuito il pattern server, gli indirizzi verranno allocati dal pool selezionato e assegnati a singole porte di adattatori.

Sono disponibili i seguenti pool predefiniti di indirizzi Fibre Channel:

- Indirizzi WWN Lenovo
- Indirizzi WWN Brocade
- Indirizzi WWN Emulex
- Indirizzi WWN QLogic

Per un elenco degli intervalli di indirizzi WWN in questi pool, vedere Pool di indirizzi (WWN) Fibre Channel.

L'intervallo di indirizzi nei pool di indirizzi deve essere univoco all'interno del dominio XClarity Administrator. XClarity Administrator garantisce che gli intervalli definiti e gli indirizzi assegnati sono univoci all'interno del relativo dominio di gestione.

Importante: In ambienti di grandi dimensioni con più istanze di XClarity Administrator, accertarsi che vengano utilizzati intervalli di indirizzi univoci da ciascuna istanza di XClarity Administrator per evitare indirizzi duplicati.

I pool di indirizzi Ethernet e Fibre Channel vengono utilizzati con l'indirizzamento virtuale degli adattatori I/O per assegnare indirizzi I/O univoci all'interno dell'organizzazione. Quando si crea un pattern server per un nodo di elaborazione, è possibile abilitare l'indirizzamento virtuale nell'ambito della configurazione dei dispositivi e degli adattatori I/O. Se l'indirizzamento virtuale è abilitato, gli indirizzi vengono assegnati dai pool di indirizzi Ethernet e Fibre Channel per evitare conflitti negli indirizzi.

Limitazione: l'indirizzamento virtuale è supportato solo per i nodi di elaborazione Flex System. Non sono supportati i server rack e tower autonomi.

Per informazioni sulla creazione di pattern server, vedere Creazione di un pattern server.

Creazione di un pool di indirizzi IP

Un *pool di indirizzi IP* definisce un intervallo di indirizzi IP per l'utilizzo durante la configurazione dell'interfaccia di rete del controller di gestione della scheda di base dei server. Una volta distribuito il pattern server associato, gli indirizzi IP vengono allocati dal pool specificato e assegnati ai singoli server.

Informazioni su questa attività

I dati nella tabella "Informazioni complessive sulla rete" nella finestra di dialogo Nuovo pool di indirizzi IP vengono ricavati dalla maschera di sottorete e dal gateway specificati o dall'intervallo iniziale. È possibile creare pool di dimensioni diverse in base alla maschera di sottorete specifica, ma gli intervalli globali dei pool devono essere univoci all'interno del dominio di gestione. Gli intervalli vengono quindi creati dall'intervallo globale del pool. Tutti gli intervalli devono essere parte della stessa sottorete e vincolati dalle restrizioni visualizzate nella tabella "Informazioni complessive sulla rete".

L'ambito di pool e intervalli è Lenovo XClarity Administrator. Nei grandi ambienti con più istanze XClarity Administrator, creare intervalli e pool univoci per ogni XClarity Administrator, in modo da evitare conflitti di indirizzo e conflitti di indirizzo con gli strumenti esistenti di gestione degli IP. Gli intervalli possono essere utilizzati anche per separate gli host (ad esempio, per tipo di sistema operativo, tipo di carico di lavoro e funzione aziendale) e per collegare le regole di rete delle organizzazioni.

Procedura

Per creare un pool di indirizzi IP, completare i seguenti passaggi.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Pool di indirizzi**. Viene visualizzata la pagina Pattern di configurazione: Pool di indirizzi.

Passo 2. Fare clic sulla scheda **Pool di indirizzi IP**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la finestra di dialogo Creazione guidata nuovi pool di indirizzi IP.

Passo 4. Fornire le seguenti informazioni.

- Nome e descrizione del pool di indirizzi.
- Scegliere se utilizzare gli indirizzi IPv4 o IPv6.
- Selezionare una maschera di sottorete (per IPv4) o una lunghezza del prefisso di instradamento (per IPv6).
- Specificare l'indirizzo gateway.I valori delle informazioni di rete vengono ricavati dal gateway e dalla maschera di sottorete specificati o dall'intervallo iniziale e inseriti nella tabella.
- Aggiungere uno o più intervalli di indirizzi:
  1. Fare clic su **Aggiungi intervallo** per aggiungere un intervallo di indirizzi. Viene visualizzata la finestra di dialogo Aggiungi nuovo intervallo di indirizzi IP.
  2. Immettere il nome dell'intervallo, l'indirizzo e le dimensioni dell'intervallo.L'ultimo indirizzo viene calcolato automaticamente.
  3. Fare clic su **OK**.L'intervallo viene aggiunto alla tabella **Definisci intervalli di indirizzi IP nei pool** e i campi nella sezione di riepilogo vengono aggiornati automaticamente.

  È possibile modificare l'intervallo facendo clic sull'icona **Modifica** ( ) oppure rimuovere l'intervallo facendo clic sull'icona **Rimuovi** ( ).

Passo 5. Fare clic su **Crea**.

Al termine

Il nuovo pool di indirizzi IP viene riportato nella tabella della pagina "Pool di indirizzi IP":

Da questa pagina, è possibile eseguire le seguenti azioni su un pool di indirizzi selezionato:

- Modificare il pool di indirizzi facendo clic sull'icona **Modifica** ( ).
- Rinominare il pool di indirizzi facendo clic sull'icona **Rinomina**.
- Eliminare il pool di indirizzi facendo clic sull'icona **Elimina** ( ).
- Visualizza i dettagli sul pool di indirizzi, come un'associazione tra gli indirizzi virtuali e le porte dell'adattatore installato e gli indirizzi virtuali riservati, facendo clic sul nome del pool nella colonna **Nome pool**.

Creazione di un pool di indirizzi Ethernet

I *pool di indirizzi Ethernet* sono raccolte di indirizzi MAC (Media Access Control) univoci che possono essere assegnati alle schede di rete. È possibile utilizzare o personalizzare pool di indirizzi predefiniti oppure è possibile crearne nuovi in base alle esigenze. Una volta creato un pattern server, se si abilita l'indirizzamento

virtuale per gli adattatori Ethernet, è possibile scegliere il pool di indirizzi Ethernet da utilizzare quando il pattern viene distribuito. Una volta distribuito il pattern server associato, gli indirizzi MAC vengono allocati dal pool di indirizzi selezionati e assegnati ai singoli adattatori di rete dei server.

Procedura

Per creare un pool di indirizzi Ethernet, completare i seguenti passaggi.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pool di indirizzi**. Viene visualizzata la pagina Pattern di configurazione: Pool di indirizzi.

Passo 2. Fare clic sulla scheda **Pool di indirizzi Ethernet**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la finestra di dialogo Nuovi pool di indirizzi Ethernet (MAC).

Passo 4. Immettere il nome e la descrizione del pool di indirizzi.

Passo 5. Aggiungere uno o più intervalli di indirizzi:

a. Fare clic su **Aggiungi intervallo** per aggiungere un intervallo di indirizzi. Viene visualizzata la finestra di dialogo "Intervallo di indirizzi Ethernet (MAC)".

b. Immettere il nome dell'intervallo, il primo indirizzo MAC e le dimensioni dell'intervallo.

L'ultimo indirizzo MAC viene calcolato automaticamente.

c. Fare clic su **Aggiungi**.

L'intervallo viene aggiunto alla tabella **Definisci intervalli di indirizzi pool Ethernet (MAC)** e i campi nella sezione di riepilogo vengono aggiornati automaticamente.

È possibile modificare l'intervallo facendo clic sull'icona **Modifica** ( ) oppure rimuovere l'intervallo facendo clic sull'icona **Rimuovi** ( ).

Passo 6. Fare clic su **Salva**.

Al termine

Il nuovo pool di indirizzi Ethernet viene riportato nella pagina "Pool di indirizzi Ethernet".

Da questa pagina, è possibile eseguire le seguenti azioni su un pool di indirizzi selezionato:

- Modificare il pool di indirizzi facendo clic sull'icona **Modifica** ( ).
- Rinominare il pool di indirizzi facendo clic sull'icona **Rinomina**.

- Eliminare il pool di indirizzi facendo clic sull'icona **Elimina** ().
- Visualizza i dettagli sul pool di indirizzi, come un'associazione tra gli indirizzi virtuali e le porte dell'adattatore installato e gli indirizzi virtuali riservati, facendo clic sul nome del pool nella colonna **Nome pool**.

Pool di indirizzi Ethernet (MAC)

I pool di indirizzi Ethernet sono raccolte di indirizzi MAC (Media Access Control) univoci che possono essere assegnati alle schede di rete. È possibile utilizzare il seguente pool di indirizzi predefiniti nei pattern server.

Tabella 3. Pool di indirizzi MAC Lenovo

Intervallo predefinito	Indirizzo iniziale	Indirizzo finale
Intervallo 1	00:1A:64:76:00:00	00:1A:64:76:1C:70
Intervallo 2	00:1A:64:76:1C:71	00:1A:64:76:38:E1
Intervallo 3	00:1A:64:76:38:E2	00:1A:64:76:55:52
Intervallo 4	00:1A:64:76:55:53	00:1A:64:76:71:C3
Intervallo 5	00:1A:64:76:71:C4	00:1A:64:76:8E:34
Intervallo 6	00:1A:64:76:8E:35	00:1A:64:76:AA:A5
Intervallo 7	00:1A:64:76:AA:A6	00:1A:64:76:C7:16
Intervallo 8	00:1A:64:76:C7:17	00:1A:64:76:E3:87
Intervallo 9	00:1A:64:76:E3:88	00:1A:64:76:FF:F8

Creazione di un pool di indirizzi Fibre Channel

I *pool di indirizzi Fibre Channel* sono raccolte di indirizzi WWNN (World Wide Node Name) e WWPN (World Wide Port Name) univoci che possono essere assegnati agli adattatori Fibre Channel. È possibile utilizzare o personalizzare pool di indirizzi predefiniti oppure è possibile crearne nuovi in base alle esigenze. Una volta creati i pattern server, se si abilita l'indirizzamento virtuale per gli adattatori Ethernet, è possibile scegliere il pool di indirizzi Fibre Channel da utilizzare quando il pattern viene distribuito. Una volta distribuito il pattern server associato, gli indirizzi WWNN e WWPN vengono allocati dal pool e assegnati ai singoli server.

Procedura

Per creare un pool di indirizzi Fibre Channel, completare i seguenti passaggi.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pool di indirizzi**. Viene visualizzata la pagina Pattern di configurazione: Pool di indirizzi.

Passo 2. Fare clic sulla scheda **Pool di indirizzi Fibre Channel**.

Passo 3. Fare clic sull'icona **Crea** (). Viene visualizzata la finestra di dialogo Pool di indirizzi Fibre Channel.

Passo 4. Immettere il nome e la descrizione del pool di indirizzi.

Passo 5. Aggiungere uno o più intervalli di indirizzi:

a. Fare clic su **Aggiungi intervallo** per aggiungere un intervallo di indirizzi. Viene visualizzata la finestra di dialogo "Pool di indirizzi (WWN) Fibre Channel".

b. Immettere il nome dell'intervallo, le dimensioni dell'intervallo e il primo indirizzo di ogni fabric.

   Gli ultimi indirizzi vengono calcolati automaticamente.

c. Fare clic su **Aggiungi**.

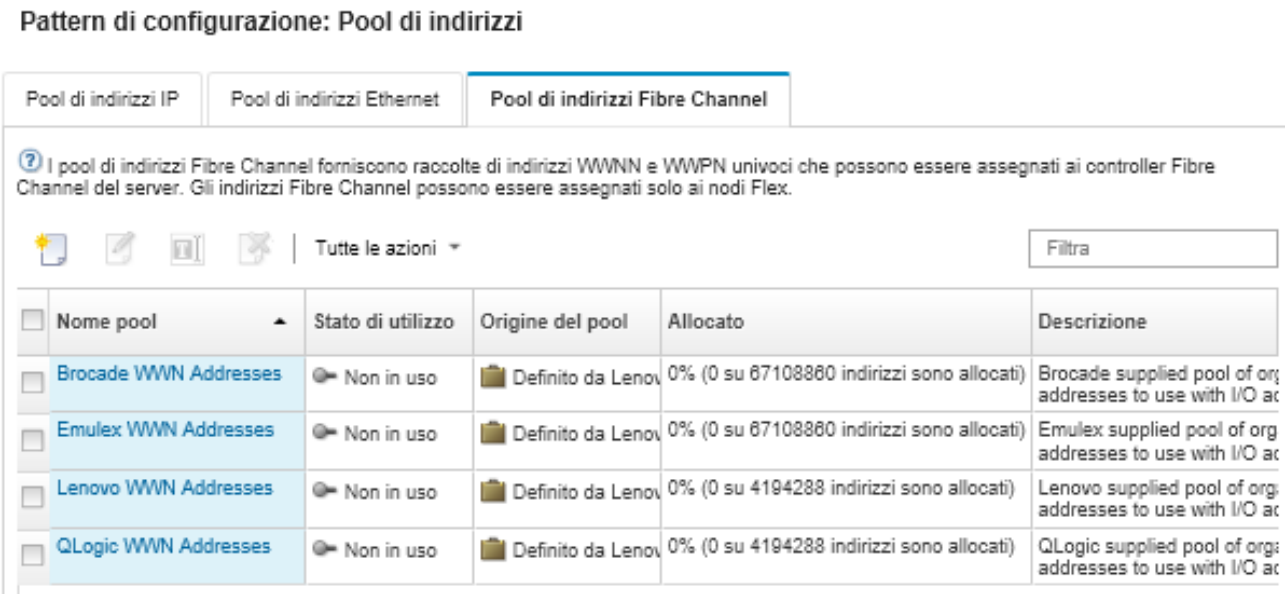
L'intervallo viene aggiunto alla tabella **Definisci intervalli di indirizzi pool Fibre Channel** e i campi nella sezione di riepilogo vengono aggiornati automaticamente.

È possibile modificare l'intervallo facendo clic sull'icona **Modifica** ( ) oppure rimuovere l'intervallo facendo clic sull'icona **Rimuovi** ( ).

Passo 6. Fare clic su **Salva**.

Al termine

Il nuovo pool di indirizzi Fibre Channel viene riportato nella tabella "Pool di indirizzi Fibre Channel":



Da questa pagina, è possibile eseguire le seguenti azioni su un pool di indirizzi selezionato:

- Modificare il pool di indirizzi facendo clic sull'icona **Modifica** ( ).
- Eliminare il pool di indirizzi facendo clic sull'icona **Elimina** ( ).
- Visualizza i dettagli sul pool di indirizzi, come un'associazione tra gli indirizzi virtuali e le porte dell'adattatore installato e gli indirizzi virtuali riservati, facendo clic sul nome del pool nella colonna **Nome pool**.

Pool di indirizzi (WWN) Fibre Channel

I pool di indirizzi Fibre Channel sono raccolte di indirizzi WWNN (World Wide Node Name, nome di nodo universale) e WWPN (World Wide Port Name, nome di porta universale) univoci che possono essere assegnati agli adattatori Fibre Channel. È possibile utilizzare i seguenti pool di indirizzi predefiniti nei pattern server.

Tabella 4 "Pool di indirizzi WWN Brocade" a pagina 337 elenca i pool di indirizzi WWN (World Wide Name) Brocade. Ogni intervallo Brocade contiene 1.864.135 indirizzi.

Tabella 5 "Pool di indirizzi WWN Emulex" a pagina 338 elenca i pool di indirizzi WWN Emulex. Ogni intervallo Emulex contiene 1.864.135 indirizzi.

Tabella 6 "Pool di indirizzi WWN Lenovo" a pagina 339 elenca i pool di indirizzi WWN Lenovo. Ogni intervallo WWN Lenovo contiene 116.508 indirizzi.

Tabella 7 "Pool di indirizzi WWN QLogic" a pagina 340 elenca i pool di indirizzi WWN QLogic. Ogni intervallo WWN QLogic contiene 116.508 indirizzi.

Tabella 4. Pool di indirizzi WWN Brocade

Intervallo predefinito	Indirizzo WWNN iniziale	Indirizzo WWNN finale	Indirizzo WWPN iniziale	Indirizzo WWPN finale
Fabric A				
Intervallo 1	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:1C:71:C6	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:1C:71:C6
Intervallo 2	2B:FA:00:05:1E:1C:71:C7	2B:FA:00:05:1E:38:E3:8D	2B:FC:00:05:1E:1C:71:C7	2B:FC:00:05:1E:38:E3:8D
Intervallo 3	2B:FA:00:05:1E:38:E3:8E	2B:FA:00:05:1E:55:55:54	2B:FC:00:05:1E:38:E3:8E	2B:FC:00:05:1E:55:55:54
Intervallo 4	2B:FA:00:05:1E:55:55:55	2B:FA:00:05:1E:71:C7:1B	2B:FC:00:05:1E:55:55:55	2B:FC:00:05:1E:71:C7:1B
Intervallo 5	2B:FA:00:05:1E:71:C7:1C	2B:FA:00:05:1E:8E:38:E2	2B:FC:00:05:1E:71:C7:1C	2B:FC:00:05:1E:8E:38:E2
Intervallo 6	2B:FA:00:05:1E:8E:38:E3	2B:FA:00:05:1E:AA:AA:A9	2B:FC:00:05:1E:8E:38:E3	2B:FC:00:05:1E:AA:AA:A9
Intervallo 7	2B:FA:00:05:1E:AA:AA:AA	2B:FA:00:05:1E:C7:1C:70	2B:FC:00:05:1E:AA:AA:AA	2B:FC:00:05:1E:C7:1C:70
Intervallo 8	2B:FA:00:05:1E:C7:1C:71	2B:FA:00:05:1E:E3:8E:37	2B:FC:00:05:1E:C7:1C:71	2B:FC:00:05:1E:E3:8E:37
Intervallo 9	2B:FA:00:05:1E:E3:8E:38	2B:FA:00:05:1E:FF:FF:FE	2B:FC:00:05:1E:E3:8E:38	2B:FC:00:05:1E:FF:FF:FE
Fabric B				
Intervallo 1	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:1C:71:C6	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:1C:71:C6
Intervallo 2	2B:FB:00:05:1E:1C:71:C7	2B:FB:00:05:1E:38:E3:8D	2B:FD:00:05:1E:1C:71:C7	2B:FD:00:05:1E:38:E3:8D
Intervallo 3	2B:FB:00:05:1E:38:E3:8E	2B:FB:00:05:1E:55:55:54	2B:FD:00:05:1E:38:E3:8E	2B:FD:00:05:1E:55:55:54
Intervallo 4	2B:FB:00:05:1E:55:55:55	2B:FB:00:05:1E:71:C7:1B	2B:FD:00:05:1E:55:55:55	2B:FD:00:05:1E:71:C7:1B
Intervallo 5	2B:FB:00:05:1E:71:C7:1C	2B:FB:00:05:1E:8E:38:E2	2B:FD:00:05:1E:71:C7:1C	2B:FD:00:05:1E:8E:38:E2
Intervallo 6	2B:FB:00:05:1E:8E:38:E3	2B:FB:00:05:1E:AA:AA:A9	2B:FD:00:05:1E:8E:38:E3	2B:FD:00:05:1E:AA:AA:A9
Intervallo 7	2B:FB:00:05:1E:AA:AA:AA	2B:FB:00:05:1E:C7:1C:70	2B:FD:00:05:1E:AA:AA:AA	2B:FD:00:05:1E:C7:1C:70
Intervallo 8	2B:FB:00:05:1E:C7:1C:71	2B:FB:00:05:1E:E3:8E:37	2B:FD:00:05:1E:C7:1C:71	2B:FD:00:05:1E:E3:8E:37
Intervallo 9	2B:FB:00:05:1E:E3:8E:38	2B:FB:00:05:1E:FF:FF:FE	2B:FD:00:05:1E:E3:8E:38	2B:FD:00:05:1E:FF:FF:FE

Tabella 5. Pool di indirizzi WWN Emulex

Intervallo predefinito	Indirizzo WWNN iniziale	Indirizzo WWNN finale	Indirizzo WWPN iniziale	Indirizzo WWPN finale
Fabric A				
Intervallo 1	2F:FE:00:00:C9:00:00:00	2F:FE:00:00:C9:1C:71:C6	2F:FC:00:00:C9:00:00:00	2F:FC:00:00:C9:1C:71:C6
Intervallo 2	2F:FE:00:00:C9:1C:71:C7	2F:FE:00:00:C9:38:E3:8D	2F:FC:00:00:C9:1C:71:C7	2F:FC:00:00:C9:38:E3:8D
Intervallo 3	2F:FE:00:00:C9:38:E3:8E	2F:FE:00:00:C9:55:55:54	2F:FC:00:00:C9:38:E3:8E	2F:FC:00:00:C9:55:55:54
Intervallo 4	2F:FE:00:00:C9:55:55:55	2F:FE:00:00:C9:71:C7:1B	2F:FC:00:00:C9:55:55:55	2F:FC:00:00:C9:71:C7:1B
Intervallo 5	2F:FE:00:00:C9:71:C7:1C	2F:FE:00:00:C9:8E:38:E2	2F:FC:00:00:C9:71:C7:1C	2F:FC:00:00:C9:8E:38:E2
Intervallo 6	2F:FE:00:00:C9:8E:38:E3	2F:FE:00:00:C9:AA:AA:A9	2F:FC:00:00:C9:8E:38:E3	2F:FC:00:00:C9:AA:AA:A9
Intervallo 7	2F:FE:00:00:C9:AA:AA:AA	2F:FE:00:00:C9:C7:1C:70	2F:FC:00:00:C9:AA:AA:AA	2F:FC:00:00:C9:C7:1C:70
Intervallo 8	2F:FE:00:00:C9:C7:1C:71	2F:FE:00:00:C9:E3:8E:37	2F:FC:00:00:C9:C7:1C:71	2F:FC:00:00:C9:E3:8E:37
Intervallo 9	2F:FE:00:00:C9:E3:8E:38	2F:FE:00:00:C9:FF:FF:FE	2F:FC:00:00:C9:E3:8E:38	2F:FC:00:00:C9:FF:FF:FE
Fabric B				
Intervallo 1	2F:FF:00:00:C9:00:00:00	2F:FF:00:00:C9:1C:71:C6	2F:FD:00:00:C9:00:00:00	2F:FD:00:00:C9:1C:71:C6
Intervallo 2	2F:FF:00:00:C9:1C:71:C7	2F:FF:00:00:C9:38:E3:8D	2F:FD:00:00:C9:1C:71:C7	2F:FD:00:00:C9:38:E3:8D
Intervallo 3	2F:FF:00:00:C9:38:E3:8E	2F:FF:00:00:C9:55:55:54	2F:FD:00:00:C9:38:E3:8E	2F:FD:00:00:C9:55:55:54
Intervallo 4	2F:FF:00:00:C9:55:55:55	2F:FF:00:00:C9:71:C7:1B	2F:FD:00:00:C9:55:55:55	2F:FD:00:00:C9:71:C7:1B
Intervallo 5	2F:FF:00:00:C9:71:C7:1C	2F:FF:00:00:C9:8E:38:E2	2F:FD:00:00:C9:71:C7:1C	2F:FD:00:00:C9:8E:38:E2
Intervallo 6	2F:FF:00:00:C9:8E:38:E3	2F:FF:00:00:C9:AA:AA:A9	2F:FD:00:00:C9:8E:38:E3	2F:FD:00:00:C9:AA:AA:A9
Intervallo 7	2F:FF:00:00:C9:AA:AA:AA	2F:FF:00:00:C9:C7:1C:70	2F:FD:00:00:C9:AA:AA:AA	2F:FD:00:00:C9:C7:1C:70
Intervallo 8	2F:FF:00:00:C9:C7:1C:71	2F:FF:00:00:C9:E3:8E:37	2F:FD:00:00:C9:C7:1C:71	2F:FD:00:00:C9:E3:8E:37
Intervallo 9	2F:FF:00:00:C9:E3:8E:38	2F:FF:00:00:C9:FF:FF:FE	2F:FD:00:00:C9:E3:8E:38	2F:FD:00:00:C9:FF:FF:FE

Tabella 6. Pool di indirizzi WWN Lenovo

Intervallo predefinito	Indirizzo WWNN iniziale	Indirizzo WWNN finale	Indirizzo WWPN iniziale	Indirizzo WWPN finale
Fabric A				
Intervallo 1	20:80:00:50:76:00:00:00	20:80:00:50:76:01:C7:1B	21:80:00:50:76:00:00:00	21:80:00:50:76:01:C7:1B
Intervallo 2	20:80:00:50:76:01:C7:1C	20:80:00:50:76:03:8E:37	21:80:00:50:76:01:C7:1C	21:80:00:50:76:03:8E:37
Intervallo 3	20:80:00:50:76:03:8E:38	20:80:00:50:76:05:55:53	21:80:00:50:76:03:8E:38	21:80:00:50:76:05:55:53
Intervallo 4	20:80:00:50:76:05:55:54	20:80:00:50:76:07:1C:6F	21:80:00:50:76:05:55:54	21:80:00:50:76:07:1C:6F
Intervallo 5	20:80:00:50:76:07:1C:70	20:80:00:50:76:08:E3:8B	21:80:00:50:76:07:1C:70	21:80:00:50:76:08:E3:8B
Intervallo 6	20:80:00:50:76:08:E3:8C	20:80:00:50:76:0A:AA:A7	21:80:00:50:76:08:E3:8C	21:80:00:50:76:0A:AA:A7
Intervallo 7	20:80:00:50:76:0A:AA:A8	20:80:00:50:76:0C:71:C3	21:80:00:50:76:0A:AA:A8	21:80:00:50:76:0C:71:C3
Intervallo 8	20:80:00:50:76:0C:71:C4	20:80:00:50:76:0E:38:DF	21:80:00:50:76:0C:71:C4	21:80:00:50:76:0E:38:DF
Intervallo 9	20:80:00:50:76:0E:38:E0	20:80:00:50:76:0F:FF:FB	21:80:00:50:76:0E:38:E0	21:80:00:50:76:0F:FF:FB
Fabric B				
Intervallo 1	20:81:00:50:76:20:00:00	20:81:00:50:76:21:C7:1B	21:81:00:50:76:20:00:00	21:81:00:50:76:21:C7:1B
Intervallo 2	20:81:00:50:76:21:C7:1C	20:81:00:50:76:23:8E:37	21:81:00:50:76:21:C7:1C	21:81:00:50:76:23:8E:37
Intervallo 3	20:81:00:50:76:23:8E:38	20:81:00:50:76:25:55:53	21:81:00:50:76:23:8E:38	21:81:00:50:76:25:55:53
Intervallo 4	20:81:00:50:76:25:55:54	20:81:00:50:76:27:1C:6F	21:81:00:50:76:25:55:54	21:81:00:50:76:27:1C:6F
Intervallo 5	20:81:00:50:76:27:1C:70	20:81:00:50:76:28:E3:8B	21:81:00:50:76:27:1C:70	21:81:00:50:76:28:E3:8B
Intervallo 6	20:81:00:50:76:28:E3:8C	20:81:00:50:76:2A:AA:A7	21:81:00:50:76:28:E3:8C	21:81:00:50:76:2A:AA:A7
Intervallo 7	20:81:00:50:76:2A:AA:A8	20:81:00:50:76:2C:71:C3	21:81:00:50:76:2A:AA:A8	21:81:00:50:76:2C:71:C3
Intervallo 8	20:81:00:50:76:2C:71:C4	20:81:00:50:76:2E:38:DF	21:81:00:50:76:2C:71:C4	21:81:00:50:76:2E:38:DF
Intervallo 9	20:81:00:50:76:2E:38:E0	20:81:00:50:76:2F:FF:FB	21:81:00:50:76:2E:38:E0	21:81:00:50:76:2F:FF:FB

Tabella 7. Pool di indirizzi WWN QLogic

Intervallo predefinito	Indirizzo WWNN iniziale	Indirizzo WWNN finale	Indirizzo WWPN finale	Indirizzo WWPN finale
Fabric A				
Intervallo 1	20:80:00: E0:8B:00:00:00	20:80:00:E0:8B:01: C7:1B	21:80:00: E0:8B:00:00:00	21:80:00:E0:8B:01: C7:1B
Intervallo 2	20:80:00:E0:8B:01: C7:1C	20:80:00: E0:8B:03:8E:37	21:80:00:E0:8B:01: C7:1C	21:80:00: E0:8B:03:8E:37
Intervallo 3	20:80:00: E0:8B:03:8E:38	20:80:00: E0:8B:05:55:53	21:80:00: E0:8B:03:8E:38	21:80:00: E0:8B:05:55:53
Intervallo 4	20:80:00: E0:8B:05:55:54	20:80:00: E0:8B:07:1C:6F	21:80:00: E0:8B:05:55:54	21:80:00: E0:8B:07:1C:6F
Intervallo 5	20:80:00: E0:8B:07:1C:70	20:80:00:E0:8B:08: E3:8B	21:80:00: E0:8B:07:1C:70	21:80:00:E0:8B:08: E3:8B
Intervallo 6	20:80:00:E0:8B:08: E3:8C	20:80:00:E0:8B:0A:AA: A7	21:80:00:E0:8B:08: E3:8C	21:80:00:E0:8B:0A:AA: A7
Intervallo 7	20:80:00:E0:8B:0A:AA: A8	20:80:00:E0:8B:0C:71: C3	21:80:00:E0:8B:0A:AA: A8	21:80:00:E0:8B:0C:71: C3
Intervallo 8	20:80:00:E0:8B:0C:71: C4	20:80:00:E0:8B:0E:38: DF	21:80:00:E0:8B:0C:71: C4	21:80:00:E0:8B:0E:38: DF
Intervallo 9	20:80:00:E0:8B:0E:38: E0	20:80:00:E0:8B:0F:FF: FB	21:80:00:E0:8B:0E:38: E0	21:80:00:E0:8B:0F:FF: FB
Fabric B				
Intervallo 1	20:81:00: E0:8B:20:00:00	20:81:00:E0:8B:21: C7:1B	21:81:00: E0:8B:20:00:00	21:81:00:E0:8B:21: C7:1B
Intervallo 2	20:81:00:E0:8B:21: C7:1C	20:81:00: E0:8B:23:8E:37	21:81:00:E0:8B:21: C7:1C	21:81:00: E0:8B:23:8E:37
Intervallo 3	20:81:00: E0:8B:23:8E:38	20:81:00: E0:8B:25:55:53	21:81:00: E0:8B:23:8E:38	21:81:00: E0:8B:25:55:53
Intervallo 4	20:81:00: E0:8B:25:55:54	20:81:00: E0:8B:27:1C:6F	21:81:00: E0:8B:25:55:54	21:81:00: E0:8B:27:1C:6F
Intervallo 5	20:81:00: E0:8B:27:1C:70	20:81:00:E0:8B:28: E3:8B	21:81:00: E0:8B:27:1C:70	21:81:00:E0:8B:28: E3:8B
Intervallo 6	20:81:00:E0:8B:28: E3:8C	20:81:00:E0:8B:2A:AA: A7	21:81:00:E0:8B:28: E3:8C	21:81:00:E0:8B:2A:AA: A7
Intervallo 7	20:81:00:E0:8B:2A:AA: A8	20:81:00:E0:8B:2C:71: C3	21:81:00:E0:8B:2A:AA: A8	21:81:00:E0:8B:2C:71: C3
Intervallo 8	20:81:00:E0:8B:2C:71: C4	20:81:00:E0:8B:2E:38: DF	21:81:00:E0:8B:2C:71: C4	21:81:00:E0:8B:2E:38: DF
Intervallo 9	20:81:00:E0:8B:2E:38: E0	20:81:00:E0:8B:2F:FF: FB	21:81:00:E0:8B:2E:38: E0	21:81:00:E0:8B:2F:FF: FB

Utilizzo di pattern server

Un *pattern server* rappresenta la configurazione server precedente all'installazione del sistema operativo, che include storage locale, adattatori I/O, avvio SAN e altre impostazioni firmware del controller di gestione della scheda di base e UEFI (Unified Extensible Firmware Interface). I pattern server integrano inoltre il supporto

per la virtualizzazione degli indirizzi I/O, pertanto è possibile virtualizzare le connessioni fabric del server oppure reimpiegare i server senza interruzione. Un pattern server viene utilizzato come pattern globale per configurare rapidamente più server alla volta.

Informazioni su questa attività

È possibile definire più pattern server per rappresentare configurazioni diverse utilizzate nel centro dati.

In fase di definizione di un pattern server, selezionare o creare pattern categoria e pool di indirizzi in base alle esigenze per creare la configurazione desiderata per un gruppo specifico di server. Un *pattern categoria* definisce le impostazioni firmware specifiche che possono essere riutilizzate da più pattern server. I pool di indirizzi consentono di definire intervalli da utilizzare per assegnare indirizzi a singoli server durante la distribuzione di pattern server. Sono disponibili pool di indirizzi IP, pool di indirizzi Ethernet (MAC) e pool di indirizzi Fibre Channel (WWN).

Se un pattern server viene distribuito in più server, verranno automaticamente generati più profili (un profilo per ciascun server). Ogni profilo eredita le impostazioni dal pattern server principale, per consentire di controllare una configurazione comune da un'unica posizione.

È possibile creare un pattern server da zero, definendo la configurazione desiderata prima di ricevere l'hardware. In alternativa, è possibile creare un pattern server da un server esistente e quindi utilizzarlo per il provisioning dei server rimanenti. Se si crea un pattern server da un server esistente, dalle impostazioni correnti del server vengono ricavati e creati dinamicamente pattern categoria estesi. È possibile modificare le impostazioni di categoria direttamente dai pattern server.

Attenzione: In caso di creazione di un pattern server da zero, è necessario definire le impostazioni di avvio per i server. Se si distribuisce il pattern nei server, l'ordine di avvio esistente nei server verrà sovrascritto dalle relative impostazioni predefinite nel pattern server. Se i server non si avviano in seguito alla distribuzione di un pattern server, il problema potrebbe essere riconducibile al fatto che le impostazioni di avvio originali sono state sovrascritte dalle impostazioni dell'ordine di avvio predefinite nel nuovo pattern server. Per ripristinare le impostazioni di avvio originali nei server, vedere Ripristino delle impostazioni di avvio in seguito alla distribuzione di pattern server.

Importante: Accertarsi di creare pattern server per ciascun tipo di server. Ad esempio, creare un pattern server per tutti i nodi di elaborazione x240 Flex System e un altro pattern server per tutti i nodi di elaborazione x440 Flex System. Non distribuire in un tipo di server un pattern creato per un altro tipo.

Importante: Se il nodo di gestione è guasto, potrebbe verificarsi la perdita dei pattern server. Eseguire sempre il backup del software di gestione dopo aver creato o modificato pattern server (vedere Backup di Lenovo XClarity Administrator).

Impostazioni per i dispositivi di rete

Alcuni dispositivi di rete Flex System offrono più opzioni di configurazione nei pattern server rispetto ad altri.

Sebbene i pattern server possano essere applicati a qualsiasi dispositivo di rete, alcune funzionalità sono limitate a specifiche schede di rete. Non sono inoltre al momento supportate alcune impostazioni avanzate per schede di rete Ethernet (ad esempio, le preferenze di compatibilità di adattatori e porte).

I pattern server possono ricavare dati e impostazioni delle configurazioni esistenti per le schede di rete supportate e possono modificare le impostazioni di configurazione tramite la distribuzione dei pattern.

Pattern categoria

Le impostazioni firmware sono organizzate in categorie che raggruppano le impostazioni correlate. Per ciascun categoria è possibile creare un *pattern categoria* che contiene le impostazioni firmware comuni e può essere riutilizzato da più pattern server. La maggior parte delle impostazioni firmware che è possibile configurare direttamente nel controller di gestione della scheda di base e nell'interfaccia UEFI può essere configurata anche tramite pattern categoria. Le impostazioni firmware disponibili dipendono dal tipo di server, dall'ambiente Flex System e dall'ambito del pattern server.

È possibile creare pattern categoria separatamente dai pattern server.

I pattern categoria possono essere predefiniti, ricavati da server esistenti o definiti dall'utente.

- **Pattern categoria estesi**

  I *pattern categoria estesi* sono pattern per alcune impostazioni di porte di adattatori I/O, UEFI avanzate e controller di gestione della scheda di base ricavati e creati dinamicamente da uno specifico server gestito. Lenovo XClarity Administrator crea questi pattern contestualmente al pattern server da un server esistente. Non è possibile creare manualmente pattern categoria estesi, ma sarà possibile modificare i pattern dopo averli creati.

  I seguenti pattern UEFI estesi vengono predefiniti da XClarity Administrator per ottimizzare i server per ambienti specifici.
  - **Opzioni di installazione ESXi**
  - **Efficienza - Prestazioni preferite**
  - **Efficienza - Alimentazione preferita**
  - **Prestazioni massime**
  - **Alimentazione minima**
- **Pattern categoria definiti dall'utente**

  I *pattern categoria definiti dall'utente* sono pattern che è possibile creare, tra cui informazioni di sistema, interfacce di gestione, dispositivi e porte I/O, destinazioni di avvio Fibre Channel e porte di adattatori I/O. È possibile creare i seguenti pattern categoria:

  - **Informazioni di sistema**. Le impostazioni comprendono nome di sistema, posizione e contatti generati automaticamente,
  - **Interfaccia di gestione**. Le impostazioni includono nome host, indirizzo IP, spazio dei nomi di dominio (DNS), velocità dell'interfaccia e assegnazioni di porte generati automaticamente per l'interfaccia di gestione.Le impostazioni duplex non sono supportate dai pattern server.
  - **Dispositivi e porte I/O**. Le impostazioni includono il reindirizzamento della console e le porte COM. È possibile utilizzare pattern server per abilitare il servizio SOL (Serial Over LAN) nell'area di reindirizzamento della console. Tuttavia, se SOL (Serial Over LAN) è abilitato, l'unica impostazione di modalità di accesso alle porte seriali supportata dai pattern server è **Dedicato**; le impostazioni IMPI **Condiviso** e **Pre-avvio** per la modalità di accesso alle porte seriali non sono disponibili nei pattern server.

    Importante: Se si crea un pattern server da un server esistente e per tale server è configurata l'impostazione di accesso alle porte seriali **Condiviso** o **Pre-avvio**, per il pattern Dispositivo e porte I/O ricavato dal server è configurata l'impostazione di modalità di accesso alle porte seriali **Dedicato**.
  - **Pattern di destinazione avvio Fibre Channel**. Le impostazioni includono specifiche destinazioni di avvio Fibre Channel WWN principali e secondarie.
  - **Porte**. Le impostazioni includono adattatori I/O e porte per la configurazione di interconnessioni fabric.

Creazione di un pattern server

Quando si crea un pattern server vengono definite le caratteristiche della configurazione di un tipo specifico di server. È possibile creare un pattern server da zero utilizzando le impostazioni predefinite o di un server esistente.

Informazioni su questa attività

Prima di creare un pattern server, tenere presente i seguenti suggerimenti.

- La prima volta che si crea un pattern server, considerare la possibilità di crearlo da un server esistente. Quando si crea un pattern server da un server esistente, Lenovo XClarity Administrator apprende e crea pattern categoria estesi per alcune porte di adattatore I/O, UEFI e impostazioni del controller di gestione della scheda di base. Quindi, questi pattern categoria possono essere utilizzati in qualsiasi pattern server creato successivamente. Per ulteriori informazioni sui pattern categoria, vedere Definizione delle impostazioni firmware.
- Identificare i gruppi di server con le stesse opzioni hardware e che si desidera configurare allo stesso modo. È possibile utilizzare un pattern server per applicare le stesse impostazioni di configurazione a più server, in modo da controllare una configurazione comune da un singolo luogo.
- Identificare gli aspetti della configurazione che si desidera personalizzare per il pattern server (ad esempio, storage locale, adattatori di rete, impostazioni di avvio, impostazioni del controller di gestione, impostazioni UEFI).
- Non è possibile gestire gli account utente locali o configurare il server LDAP utilizzando i pattern di configurazione.

Importante: Se il nodo di gestione è guasto, potrebbe verificarsi la perdita dei pattern server. Eseguire sempre il backup del software di gestione dopo aver creato o modificato pattern server (vedere Backup di Lenovo XClarity Administrator).

Procedura

Per creare un pattern server, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Pattern di configurazione server**. Viene visualizzata la pagina Pattern di configurazione server.

Passo 2. Fare clic sulla scheda **Pattern server**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la finestra di dialogo Creazione guidata nuovo pattern server.

Passo 4. Per creare il pattern server, effettuare una delle seguenti operazioni.

- Fare clic su **Crea un nuovo pattern da un server esistente** per utilizzare le impostazioni di un server esistente. Quindi, selezionare il server gestito su cui il nuovo pattern deve essere basato dall'elenco visualizzato.

  Quando si crea un pattern server da un server esistente, XClarity Administrator apprende le impostazioni dal server gestito specificato (tra cui la porta estesa, UEFI e le impostazioni del controller di gestione) e crea dinamicamente pattern categoria in base a queste impostazioni. Se il server è completamente nuovo, Lenovo XClarity Administrator apprende le impostazioni di fabbrica. Se XClarity Administrator sta gestendo il server, XClarity Administrator utilizza le impostazioni personalizzate. È possibile personalizzare le impostazioni in maniera specifica per i server su cui si desidera distribuire questo pattern.
- Fare clic su **Crea un nuovo pattern da zero** per utilizzare le impostazioni predefinite. Quindi, selezionare il tipo di server nel campo **Fattore di forma**.

Nota: Le opzioni disponibili nelle schede restanti potrebbero variare a seconda del tipo di server per cui si crea un pattern.

Passo 5. Immettere il nome del pattern e una descrizione.

Passo 6. Per personalizzare il nome del profilo del server, selezionare l'interruttore **Personalizzato** e quindi selezionare uno o più elementi da includere nello schema di denominazione (come, testo personalizzato, nome del server e numero incrementale) e l'ordine.

Passo 7. Fare clic su **Avanti**

Passo 8. Scegliere la configurazione di storage locale da applicare quando il pattern viene distribuito a un server e fare clic su **Avanti**.

Per ulteriori informazioni sulle impostazioni dello storage locale, vedere Definizione di storage locale.

Passo 9. **Facoltativo:** modificare l'indirizzamento dell'adattatore I/O e definire gli adattatori I/O aggiuntivi in modo che corrispondano alla configurazione hardware prevista per questo pattern e fare clic su **Avanti**.

Per informazioni sulle impostazioni dell'adattatore I/O, vedere Definizione degli adattatori I/O.

Passo 10. Definire l'ordine di avvio da applicare quando questo pattern viene distribuito a un server e fare clic su **Avanti**.

Per informazioni sulle impostazioni delle destinazioni avvio SAN, vedere Definizione delle opzioni di avvio.

Passo 11. Selezionare le impostazioni firmware dall'elenco di pattern categoria esistenti.

Per creare nuovi pattern categoria, fare clic sull'icona **Crea** ( ).

Per informazioni sulle impostazioni firmware, vedere Definizione delle impostazioni firmware.

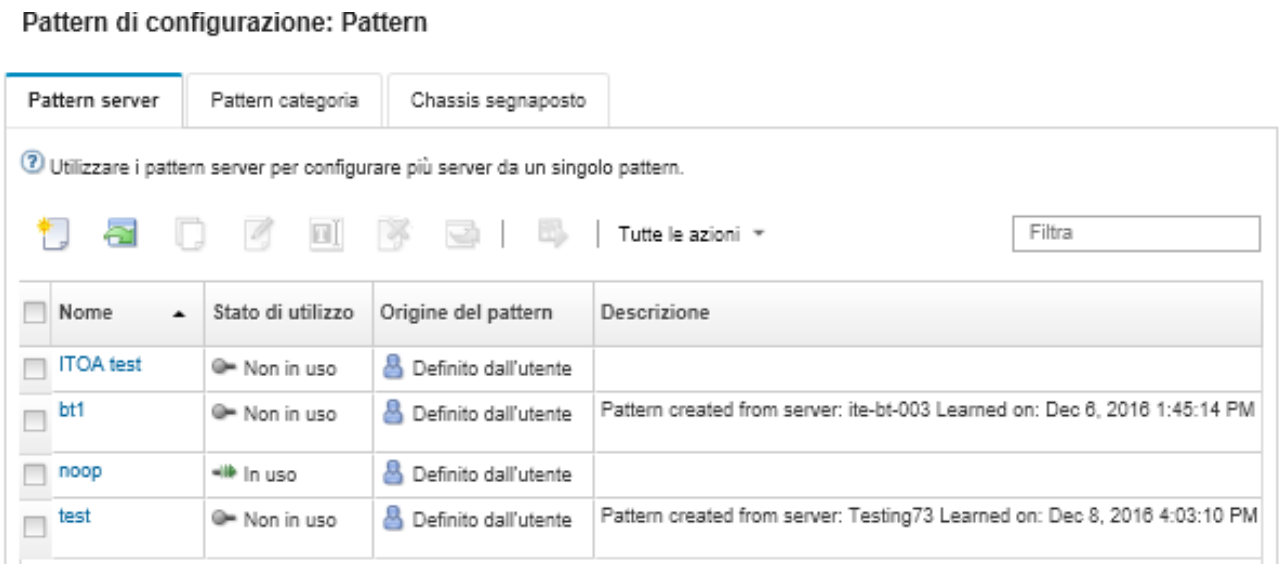
Passo 12. Fare clic su **Salva** per salvare il pattern oppure su **Salva e distribuisci** per salvare e distribuire immediatamente il pattern a uno o più server.

Per informazioni sulla distribuzione di un pattern server, vedere Distribuzione di un pattern server in un server.

Al termine

Se si è fatto clic su **Salva e distribuisci**, viene visualizzata la pagina Distribuisci pattern server. Da questa pagina, è possibile distribuire il pattern server a server specifici.

Se si è fatto clic su **Salva**, il pattern server e tutti i pattern categoria vengono salvati nella pagina Pattern server.



Da questa pagina, è possibile eseguire le seguenti azioni sui pattern server selezionati:
- Visualizzare i dettagli sul pattern facendo clic sul nome del pattern nella colonna **Nome**.
- Distribuire il pattern (vedere Distribuzione di un pattern server in un server).
- Copiare il pattern facendo clic sull'icona **Copia** ( ).
- Modificare il pattern (vedere Modifica di un pattern server).
- Rinominare il pattern, facendo clic sull'icona **Rinomina** ( ).
- Eliminare il pattern, facendo clic sull'icona **Elimina** ( ).
- Esportare e importare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Definizione di storage locale

È possibile definire la configurazione di storage locale da applicare ai server di destinazione in caso di distribuzione di questo pattern.

Informazioni su questa attività

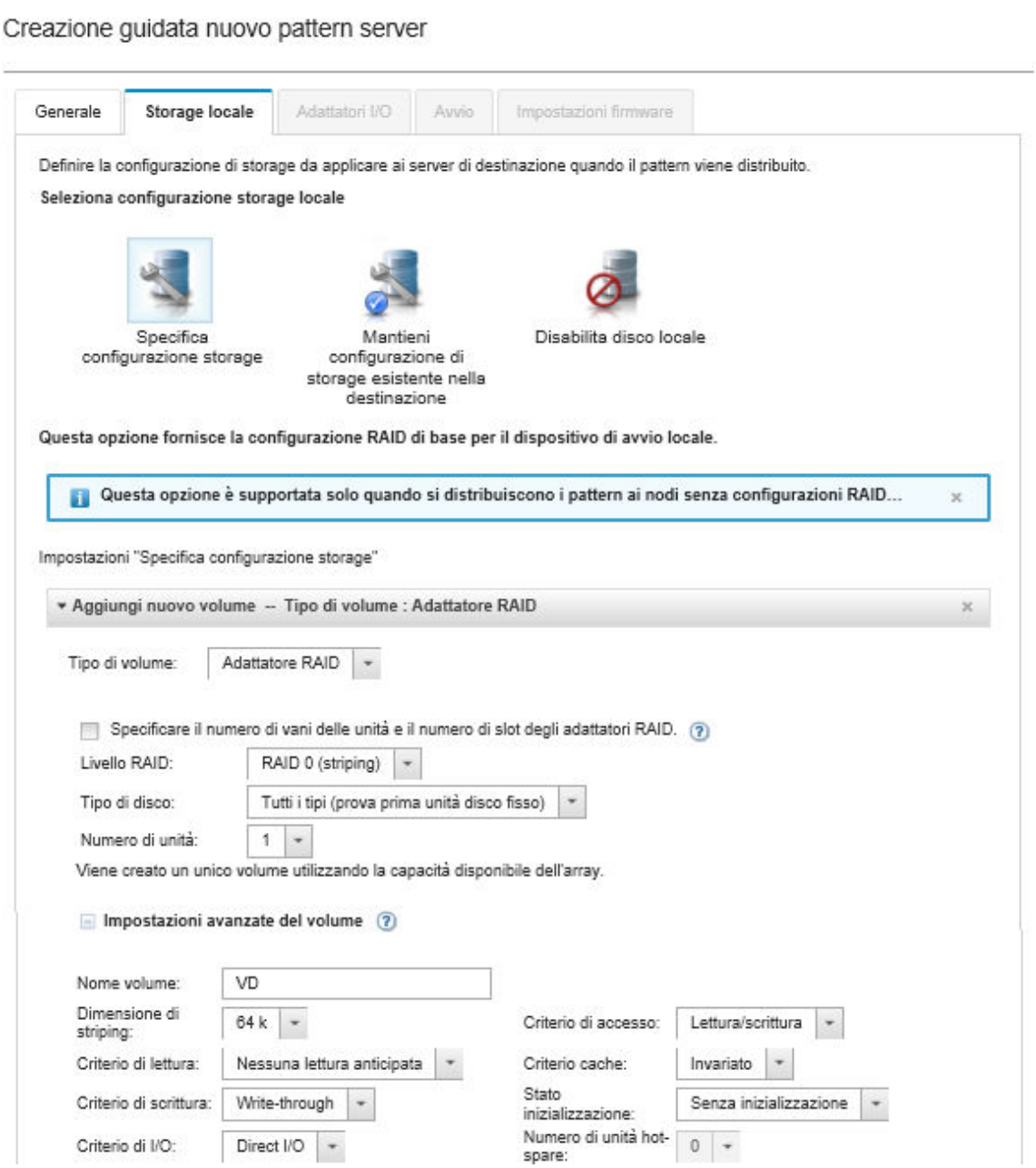
Nota:

- I controller di storage integrati nei server Flex System x220, Flex System x222 e ThinkSystem supportano configurazioni RAID basate su software. Tuttavia, la configurazione di RAID software mediante i pattern di configurazione non è supportata.
- Quando si configurano le impostazioni RAID utilizzando Pattern di configurazione, se il server è spento, il server viene avviato automaticamente con la configurazione BIOS/UEFI, prima di attivare il profilo del server.

Procedura

Per definire la configurazione di storage locale, attenersi alla procedura descritta di seguito.

Passo 1. In Creazione guidata nuovo pattern server fare clic sulla scheda **Storage locale**.



Passo 2. Per definire le impostazioni di storage locale, scegliere una delle seguenti opzioni.

- **Specifica configurazione storage**. (Solo dispositivi in configurazioni RAID) Le impostazioni RAID di base vengono configurate sul dispositivo di avvio locale durante la distribuzione

  Specificare la configurazione di storage in base all'opzione di storage. È possibile aggiungere ulteriori opzioni di storage facendo clic su **Aggiungi** ( ).

  – **Adattatore RAID**. Scegliere il livello RAID, le caratteristiche e il numero di unità installate nel server. Sono supportati i livelli RAID 0, 1 e 5. Inoltre è possibile scegliere le impostazioni avanzate del volume, come dimensioni di stripe, criteri e numero di unità hot-spare.

    Per i server ThinkSystem con XCC v2.1 e versioni successive (ThinkSystem SR950 richiede XCC 1.4 o versioni successive) è possibile specificare anche il numero di slot dell'adattatore RAID e i numeri di vani delle unità per creare un singolo volume utilizzando la capacità di array disponibile. In questo caso, sono supportati i livelli RAID 0, 1, 5, 6, 10, 50, 60 e 00.

Inoltre è possibile scegliere le impostazioni avanzate del volume, come dimensioni di stripe, criteri e unità hot-spare.

Nota: Nel server di destinazione, accertarsi che sia presente un numero sufficiente di unità del tipo specificato e che lo stato RAID delle unità sia "Bene non configurato", come riportato nella sezione **Unità** della pagina "Dettagli inventario" dei server (vedere Visualizzazione dei dettagli di un server gestito).

- **Adattatore per supporti SD Lenovo**. Scegliere la posizione in cui creare il volume e le dimensioni del volume. È anche possibile scegliere le impostazioni avanzate del volume, come il tipo di supporto e i criteri di accesso.
- **ThinkSystem M.2 con mirroring**. Scegliere lo slot PCI, il livello RAID, il nome del volume e le dimensioni di stripe per creare un singolo volume utilizzando la capacità dell'array disponibile.
  - È possibile definire più ThinkSystem M.2 con adattatori di storage per il mirroring, ciascuno in uno slot PCI diverso.
  - Per i server edge ThinkSystem, è necessario specificare un numero di slot PCI specifico. Per gli altri server ThinkSystem nei quali è installato un solo adattatore RAID M.2, è possibile scegliere il primo valore corrispondente (valore predefinito) oppure specificare un determinato numero di slot PCI.
- **Memoria persistente Intel Optane DC**. Scegliere il tipo di memoria persistente, la soglia di avvertenza per la percentuale di capacità rimanente e la percentuale di capacità totale da utilizzare come memoria. (La memoria rimanente viene utilizzata come storage persistente).

  Attenzione:
  - Per configurare i moduli DIMM di memoria persistente Intel Optane DC è necessario disabilitare la sicurezza e non creare uno spazio dei nomi.
  - L'abilitazione della sicurezza è supportata solo quando lo stato della sicurezza è "Disabilitato" per tutti i moduli DIMM di memoria persistente Intel Optane DC nel server.
  - La disabilitazione della sicurezza e la cancellazione sicura sono supportate solo quando lo stato della sicurezza è "Bloccato" e la passphrase è la stessa per tutti i moduli DIMM di memoria persistente Intel Optane DC nel server.
  - Lo stato della sicurezza Intel Optane DC PMEM non è incluso nell'inventario di XClarity Administrator. È possibile controllare manualmente lo stato della sicurezza in UEFI.

- **Mantieni configurazione di storage esistente nella destinazione**. La configurazione di storage esistente non viene modificata durante la distribuzione. Scegliere questa opzione per utilizzare la configurazione di storage esistente nel server di destinazione.
- **Disabilita disco locale**. (Solo Nodo di elaborazione Flex System x240) Il controller di storage integrato e la ROM di opzione di storage (UEFI e Legacy) sono disabilitati durante la distribuzione. La disabilitazione dell'unità disco locale riduce i tempi complessivi di avvio dalla rete SAN.

Definizione degli adattatori I/O

È possibile definire le impostazioni delle porte I/O e la modalità di indirizzamento da applicare ai server di destinazione in caso di distribuzione di questo pattern.

Informazioni su questa attività

Se si intende virtualizzare o riassegnare gli indirizzi dell'adattatore I/O, è possibile configurare questo pattern per utilizzare l'indirizzamento dell'adattatore I/O virtuale.

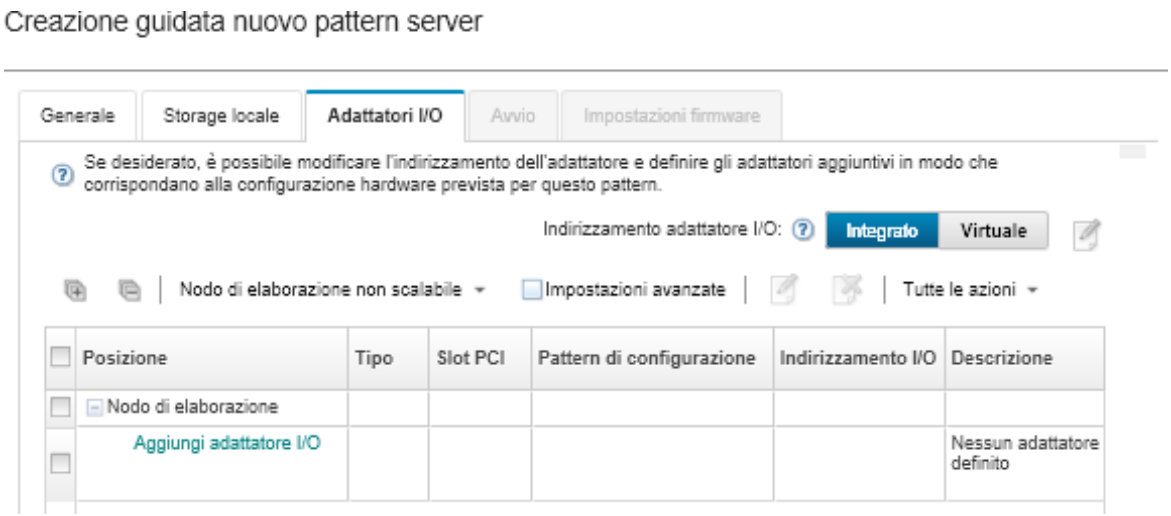
Se si sta creando un pattern da un server esistente, alcune informazioni degli adattatori potrebbero essere ereditate automaticamente. È possibile definire ulteriori pattern di adattatori I/O in modo che corrispondano

all'hardware previsto nei server in caso di distribuzione di questo pattern. Definendo i pattern degli adattatori I/O, è possibile configurare le impostazioni delle porte per l'adattatore supportato. Se si utilizzano indirizzi virtuali degli adattatori I/O, è inoltre possibile definire destinazioni di avvio SAN per gli adattatori Fibre Channel aggiunti (vedere Definizione delle opzioni di avvio).

Procedura

Per definire le impostazioni degli adattatori I/O, attenersi alla procedura descritta di seguito.

Passo 1. In Creazione guidata nuovo pattern server fare clic sulla scheda **Adattatori I/O**.



Nota: Per visualizzare informazioni aggiuntive sugli adattatori I/O, fare clic su **Impostazioni avanzate**.

Passo 2. Se si crea un pattern server per un server in uno chassis di Flex System, scegliere il tipo di modalità di indirizzamento degli adattatori I/O:

- **Integrato**. Utilizzare gli indirizzi WWN (World Wide Name, nome universale) e MAC (Media Access Control) esistenti forniti dal produttore con l'adattatore.
- **Virtuale**. Utilizzare l'indirizzamento dell'adattatore I/O virtuale per semplificare la gestione delle connessioni SAN e LAN. La virtualizzazione degli indirizzi I/O riassegna gli indirizzi hardware integrati con indirizzi WWN Fibre Channel e MAC Ethernet. In questo modo è possibile accelerare la distribuzione preconfigurando l'appartenenza alla zona SAN e agevolare il failover eliminando la necessità di riconfigurare le assegnazioni di suddivisione in zone SAN e mascheramento LUN in fase di sostituzione dell'hardware.

  Se è abilitato l'indirizzamento virtuale, gli indirizzi Ethernet e Fibre Channel sono entrambi allocati per impostazione predefinita, indipendentemente dagli adattatori definiti. È possibile scegliere il pool da cui verranno allocati gli indirizzi Ethernet e Fibre Channel.

  È inoltre possibile modificare le impostazioni degli indirizzi virtuali facendo clic sull'icona **Modifica** ( ) accanto alle modalità di indirizzamento.

  Limitazione: l'indirizzamento virtuale è supportato solo per i server in chassis di Flex System. Rack e server tower non sono supportati.

Passo 3. Se si crea un pattern server per un server in uno chassis di Flex System, selezionare una delle seguenti opzioni di scalabilità. Le righe nella tabella cambiano in base alla selezione.

- Flex System non scalabile
- Flex System scalabile a 2 nodi
- Flex System scalabile a 4 nodi

Passo 4. Scegliere gli adattatori I/O previsti per l'installazione nei server in cui verrà distribuito il pattern. Per aggiungere un adattatore:

a. Fare clic sul collegamento **Aggiungi adattatore I/O** nella tabella per visualizzare la finestra di dialogo Aggiungi adattatore I/O 1 o LOM.

b. Selezionare lo slot PCI per l'adattatore.

c. Selezionare il tipo di adattatore dalla tabella.

Nota: Per impostazione predefinita, nella tabella vengono elencati solo gli adattatori I/O attualmente installati nei server gestiti. Per un elenco di tutti gli adattatori I/O supportati, fare clic su **Tutti gli adattatori supportati**.

d. Selezionare il pattern porta iniziale da assegnare a tutte le porte nel gruppo in caso di distribuzione di questo pattern.

I *pattern porta* vengono utilizzati per modificare le impostazioni delle porte ricavate dal server. Questi pattern porta iniziali vengono assegnati in fase di aggiunta dell'adattatore. Una volta aggiunto l'adattatore, sarà possibile assegnare pattern diversi alle singole porte nella pagina degli adattatori I/O.

Per creare un pattern porta, fare clic sull'icona **Crea** ( ). Per creare un pattern porta in base a un pattern esistente, fare clic sull'icona **Modifica** ( ).

Per ulteriori informazioni sulla creazione di pattern porta, vedere Definizione delle impostazioni delle porte.

e. Fare clic su **Aggiungi** per aggiungere il pattern porta alla tabella nella pagina degli adattatori I/O.

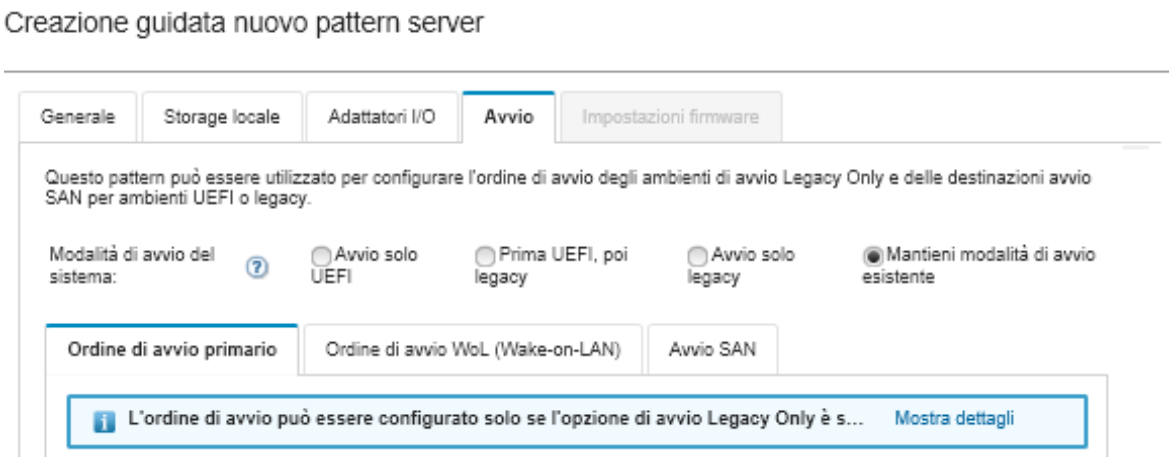
Definizione delle opzioni di avvio

È possibile definire l'ordine di avvio da applicare ai server di destinazione in caso di distribuzione di questo pattern.

Procedura

Per creare un pattern di opzioni di avvio, attenersi alla procedura descritta di seguito.

Passo 1. In Creazione guidata nuovo pattern server fare clic sulla scheda **Avvio**.



Passo 2. Selezionare una delle seguenti modalità di avvio di sistema:

- **Avvio solo UEFI**. Selezionare questa opzione per configurare un server che supporti l'interfaccia UEFI (Unified Extensible Firmware Interface). In caso di avvio di sistemi operativi abilitati per UEFI, questa opzione potrebbe ridurre i tempi di avvio disabilitando le ROM di opzione legacy.

  Se il pattern viene ricavato da un server Thinksystem, è possibile fare clic sulla scheda **Ordine di avvio primario** per specificare l'ordine di avvio. È possibile mantenere l'ordine di avvio specificato nel server in cui verrà distribuito il pattern oppure configurare l'ordine di avvio per specificare l'ordine in cui applicare le opzioni di avvio. Tuttavia, la priorità di avvio dei dispositivi di avvio in un gruppo di dispositivi (opzione di avvio) non è supportata.
- **Prima UEFI, poi legacy**. Selezionare questa opzione per configurare un server al fine di eseguire prima l'avvio con UEFI. Se si verifica un errore, il server tenterà l'avvio in modalità legacy.

  Se il pattern viene ricavato da un server Thinksystem, è possibile fare clic sulla scheda **Ordine di avvio primario** per specificare l'ordine di avvio. È possibile mantenere l'ordine di avvio specificato nel server in cui verrà distribuito il pattern oppure configurare l'ordine di avvio per specificare l'ordine in cui applicare le opzioni di avvio. Tuttavia, la priorità di avvio dei dispositivi di avvio in un gruppo di dispositivi (opzione di avvio) non è supportata.
- **Avvio solo legacy**. Selezionare questa opzione se si configura un server per l'avvio di un sistema operativo che richiede firmware (BIOS) legacy. Selezionare questa opzione solo in caso di avvio di sistemi operativi non abilitati per UEFI.

  Suggerimento: Se si seleziona la modalità Avvio solo legacy (che accelera sensibilmente i tempi di avvio), non sarà possibile attivare le chiavi FoD (Features on Demand).

  Se è stata scelta questa opzione, è possibile specificare:

  – **Ordine di avvio primario**. Scegliere questa opzione per mantenere l'ordine di avvio specificato nel server in cui verrà distribuito il pattern. È inoltre possibile scegliere di configurare l'ordine Avvio solo legacy per specificare l'ordine in cui dovranno essere applicate le opzioni di avvio.
  – **Ordine di avvio WoL (Wake-on-LAN)**. Scegliere questa opzione per mantenere l'ordine di avvio WoL corrente specificato nel server in cui verrà distribuito il pattern. È inoltre possibile scegliere di configurare l'ordine Avvio solo legacy per specificare l'ordine in cui dovranno essere applicate le opzioni di avvio WoL.
- **Mantieni modalità di avvio esistente**. Selezionare questa opzione per mantenere le impostazioni esistenti nel server di destinazione. Durante la distribuzione del pattern non verranno apportate modifiche all'ordine di avvio.

Passo 3. Selezionare la scheda **Avvio SAN** per scegliere un pattern di destinazione di avvio e specificare le destinazioni dei dispositivi di avvio.

Nota: Se in fase di definizione degli adattatori I/O sono stati definiti adattatori Fibre Channel ed è stato abilitato l'indirizzamento virtuale, è possibile impostare destinazioni di avvio SAN primarie e secondarie per gli adattatori Fibre Channel. È possibile specificare più identificatori di nome di porta universale (WWPN, World Wide Port Name) e numero di unità logica (LUN, Logical Unit Number) per le destinazioni di storage.

Definizione delle impostazioni firmware

È possibile specificare le impostazioni firmware del controller di gestione della scheda di base e UEFI (Unified Extensible Firmware Interface) da applicare ai server in caso di distribuzione di questo pattern.

Informazioni su questa attività

Le impostazioni firmware sono organizzate in categorie che raggruppano le impostazioni correlate. Per ciascun categoria è possibile creare un *pattern categoria* che contiene le impostazioni firmware comuni e può essere riutilizzato da più pattern server. La maggior parte delle impostazioni firmware che è possibile configurare direttamente nel controller di gestione della scheda di base e nell'interfaccia UEFI può essere configurata anche tramite pattern categoria. Le impostazioni firmware disponibili dipendono dal tipo di server, dall'ambiente Flex System e dall'ambito del pattern server.

I pattern categoria possono essere predefiniti, definiti dall'utente o ricavati da server esistenti:

- I *pattern categoria estesi* sono pattern per alcune impostazioni di porte di adattatori I/O, UEFI avanzate e controller di gestione della scheda di base ricavati e creati dinamicamente da uno specifico server gestito. Lenovo XClarity Administrator crea questi pattern contestualmente al pattern server da un server esistente. Non è possibile creare manualmente pattern categoria estesi, ma sarà possibile modificare i pattern dopo averli creati.
- I *pattern categoria definiti dall'utente* sono pattern che è possibile creare, tra cui informazioni di sistema, interfacce di gestione, dispositivi e porte I/O, destinazioni di avvio Fibre Channel e porte di adattatori I/O.

Procedura

Per definire le impostazioni firmware, attenersi alla procedura descritta di seguito.

Passo 1. In Creazione guidata nuovo pattern server fare clic sulla scheda **Impostazioni firmware**.

Passo 2. Scegliere il tipo di pattern categoria che includa le impostazioni da definire.

- **Informazioni di sistema**. Utilizzare questo pattern categoria per definire la generazione automatica dei nomi di sistema, i nomi di contatto e le posizioni. Per ulteriori informazioni sui pattern informazioni di sistema, vedere Definizione delle impostazioni delle informazioni di sistema.
- **Interfacce di gestione**. Utilizzare questo pattern categoria per definire la generazione automatica dei nomi host, le assegnazioni degli indirizzi IP di gestione, le impostazioni DNS (Domain Name System) e le impostazioni di velocità Internet. Per ulteriori informazioni sui pattern interfacce di gestione, vedere Definizione delle impostazioni dell'interfaccia di gestione).
- **Dispositivi e porte I/O**. Utilizzare questo pattern categoria per definire il reindirizzamento delle console e le porte COM, la velocità PCIe, i dispositivi on-board, la ROM di opzione degli

adattatori e l'ordine di esecuzione della ROM di opzione. Per ulteriori informazioni sui pattern dispositivi e porte I/O, vedere Definizione delle impostazioni di dispositivi e porte I/O.

- **BMC esteso**. Utilizzare questo pattern categoria per definire altre impostazioni del controller di gestione della scheda di base. I pattern controller di gestione esteso vengono creati automaticamente quando si crea un pattern server da un server esistente. Non è possibile creare manualmente un pattern controller di gestione esteso. Per ulteriori informazioni sui pattern interfacce di gestione, vedere Definizione delle impostazioni di controller di gestione esteso.).
- **UEFI estesa**. Utilizzare questo pattern categoria per definire altre impostazioni UEFI (Unified Extensible Firmware Interface). I pattern UEFI estesa vengono creati automaticamente quando si crea un pattern server da un server esistente. Non è possibile creare manualmente un pattern UEFI estesa. Per ulteriori informazioni sui pattern interfacce di gestione, vedere Definizione delle impostazioni UEFI estese.

Passo 3. Per creare nuovi pattern categoria, fare clic sull'icona **Crea** ( ) accanto allo specifico tipo di pattern categoria.

È inoltre possibile modificare un pattern categoria esistente selezionando un pattern specifico dall'elenco a discesa e facendo clic sull'icona **Modifica** ( ) accanto allo specifico tipo di pattern categoria. È inoltre possibile copiare un pattern categoria esistente modificandolo e facendo clic su **Salva con nome** per salvarlo con un nuovo nome.

Definizione delle impostazioni delle informazioni di sistema

È possibile definire nome di sistema, contatto e informazioni sulla posizione creando un pattern informazioni di sistema.

Procedura

Per creare un pattern informazioni di sistema, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern categoria**.

Passo 3. Fare clic sulla linguetta laterale **Pattern informazioni di sistema** e quindi sull'icona **Crea** ( ).

Suggerimento: è anche possibile creare un nuovo informazioni di sistema dalla pagina Impostazioni firmware della procedura guidata Nuovo pattern server, facendo clic sull'icona **Crea** accanto alla selezione **Informazioni di sistema**.

Passo 4. Nella finestra di dialogo Nuovo pattern informazioni di sistema, specificare le seguenti informazioni.

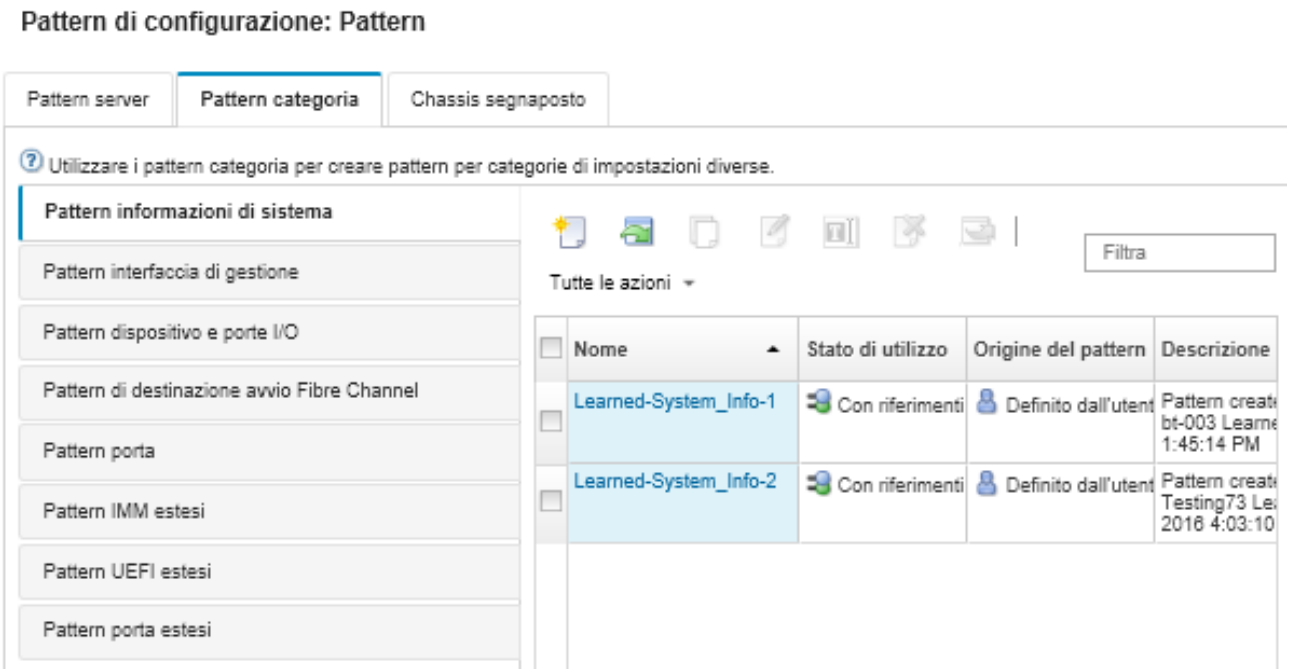
- Immettere un nome e una descrizione il pattern.
- Scegliere se generare automaticamente i nomi di sistema. Se si seleziona **Personalizzato**, è possibile specificare la modalità di generazione dei nomi quando il pattern viene distribuito. Facendo clic su **Disabilita**, il nome di sistema di ogni server non viene modificato quando il pattern viene distribuito. Per molti dispositivi, il nome è limitato a 256 caratteri latini dal controller di gestione della scheda di base. I nomi generati automaticamente vengono troncati a 256 caratteri.
- Specificare la persona da contattare per questo server e la posizione del server.

  Nota: Se SNMP è abilitato, è necessario specificare un contatto e la posizione del sistema.

Passo 5. Fare clic su **Crea**.

Risultati

Il nuovo pattern viene elencato nella scheda **Pattern informazioni di sistema** della pagina Pattern di configurazione: pattern categoria:



Da questa pagina, è anche possibile eseguire le seguenti azioni su un pattern categoria selezionato:

- Modificare le impostazioni del pattern corrente facendo clic sull'icona **Modifica** ( ).
- Copiare un pattern esistente facendo clic sull'icona **Copia** ( ).
- Eliminare un pattern facendo clic sull'icona **Elimina** ( ).
- Rinominare un pattern facendo clic sull'icona **Rinomina** ( ).
- Importare o esportare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Definizione delle impostazioni dell'interfaccia di gestione

È possibile definire nomi host, indirizzi IP, velocità dell'interfaccia DNS (Domain Name System) e assegnazioni porte per l'interfaccia di gestione, creando un pattern interfaccia di gestione.

Procedura

Per creare un pattern interfaccia di gestione, completare le seguenti operazioni.

Nota: Le impostazioni duplex non sono supportate dai pattern server.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern categoria**.

Passo 3. Fare clic sulla linguetta laterale **Pattern interfaccia di gestione**, quindi fare clic sull'icona **Crea** ( ).

Suggerimento: è anche possibile creare un nuovo pattern interfaccia di gestione dalla pagina "Impostazioni firmware" della procedura guidata Nuovo pattern server, facendo clic sull'icona **Crea** ( ) accanto alla selezione **Interfaccia di gestione**.

Passo 4. Nella finestra di dialogo Nuovo pattern interfaccia di gestione, specificare le seguenti informazioni.

- Immettere un nome e una descrizione il pattern.
- Selezionare la scheda **Nome host** e scegliere se generare automaticamente i nome host. Se si seleziona **Personalizzato**, è possibile specificare la modalità di generazione dei nomi quando il pattern viene distribuito. Facendo clic su **Disabilita**, il nome host di ogni server non viene modificato quando il pattern viene distribuito.

  I nomi host sono limitati a 63 caratteri latini dal controller di gestione della scheda di base. I nomi generati automaticamente vengono troncati a 63 caratteri.
- Fare clic sulla scheda **Indirizzi IP di gestione** e configurare le impostazioni degli indirizzi IPv4 e IPv6.

  Per gli indirizzi **IPv4**, è possibile scegliere una delle seguenti opzioni:
  - **Ottenere l'indirizzo IP dinamico dal server DHCP**.
  - **Prima da DHCP**. Se l'operazione non riesce, ottenere un indirizzo IP statico dal pool di indirizzi.
  - **Ottieni un indirizzo IP statico dal pool di indirizzi.**

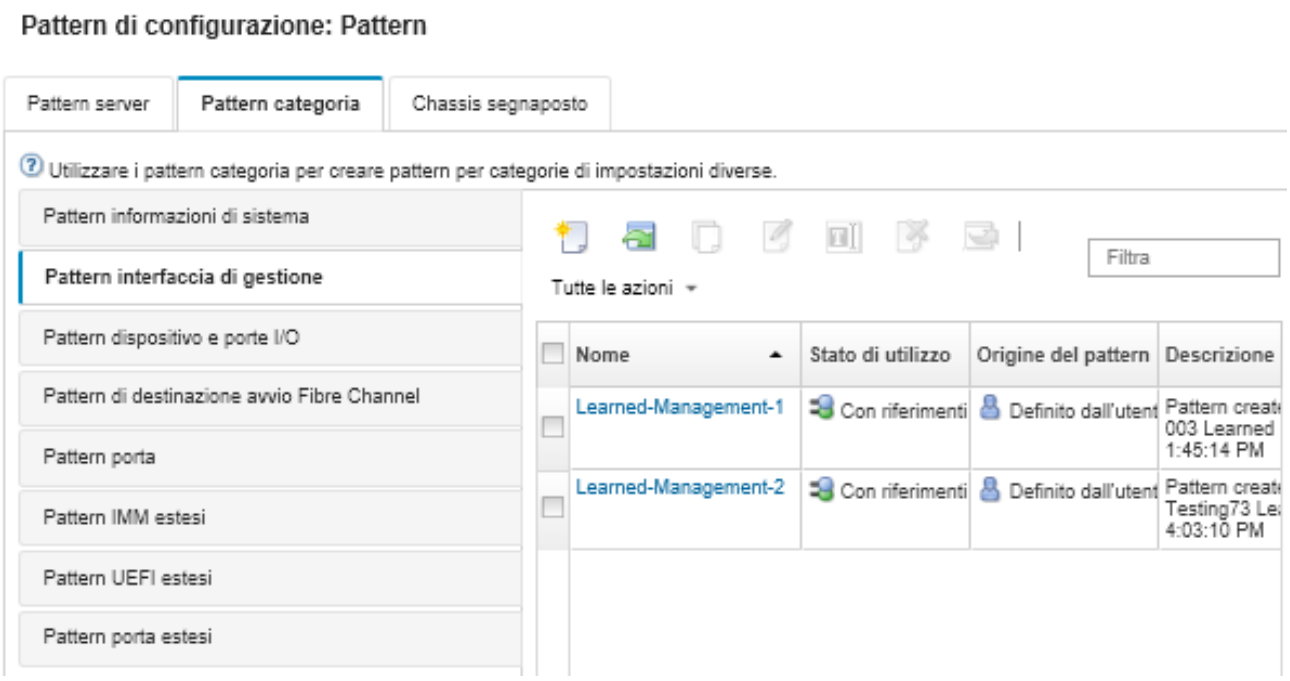
  Per gli indirizzi **IPv6**, è possibile scegliere di:
  - **Utilizzare la configurazione automatica dell'indirizzo senza stato**.
  - **Ottenere un indirizzo IP dinamico da un server DHCP**.
  - **Ottenere un indirizzo IP statico dal pool di indirizzi**.

  Nella scheda **DNS (Domain Name System)**, scegliere se abilitare o disabilitare DDNS (Dynamic Domain Name Service). Se si abilita DDNS, è possibile scegliere una delle seguenti opzioni:
  - Ottenere un nome di dominio dal server DHCP.
  - Specificare un nome di dominio.
- Fare clic sulla scheda **Impostazioni interfaccia** e specificare il valore MTU (Maximum Transmission Unit). Il valore predefinito è 1.500.
- Fare clic sulla scheda **Assegnazioni porte** e specificare i numeri per utilizzare per le seguenti porte:
  - HTTP
  - HTTPS
  - CLI Telnet
  - CLI SSH
  - Agent SNMP
  - Trap SNMP
  - Console controllo remoto
  - CIM over HTTP
  - CIM over HTTPS

Passo 5. Fare clic su **Crea**.

Risultati

Il nuovo pattern verrà elencato nella scheda **Pattern interfaccia di gestione** della pagina Pattern di configurazione: pattern categoria:



Da questa pagina, è anche possibile eseguire le seguenti azioni su un pattern categoria selezionato:

- Modificare le impostazioni del pattern corrente facendo clic sull'icona **Modifica** ( ).
- Copiare un pattern esistente facendo clic sull'icona **Copia** ( ).
- Eliminare un pattern facendo clic sull'icona **Elimina** ( ).
- Rinominare un pattern facendo clic sull'icona **Rinomina** ( ).
- Importare o esportare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Definizione delle impostazioni di dispositivi e porte I/O

È possibile abilitare il reindirizzamento della console e abilitare e definire le caratteristiche della porta COM1 creando un pattern dispositivo e porte I/O.

Procedura

Per creare un pattern dispositivo e porte I/O, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern categoria**.

Passo 3. Fare clic sulla linguetta laterale **Pattern dispositivi e porte I/O**, quindi fare clic sull'icona **Crea** ( ).

Suggerimento: è anche possibile creare un pattern dispositivi e porte I/O dalla pagina Impostazioni firmware della creazione guidata Nuovo pattern server, facendo clic sull'icona **Crea** ( ) accanto alla selezione **Pattern dispositivi e porte I/O**.

Passo 4. Nella finestra di dialogo Nuovo pattern dispositivi e porte I/O, specificare le seguenti informazioni.

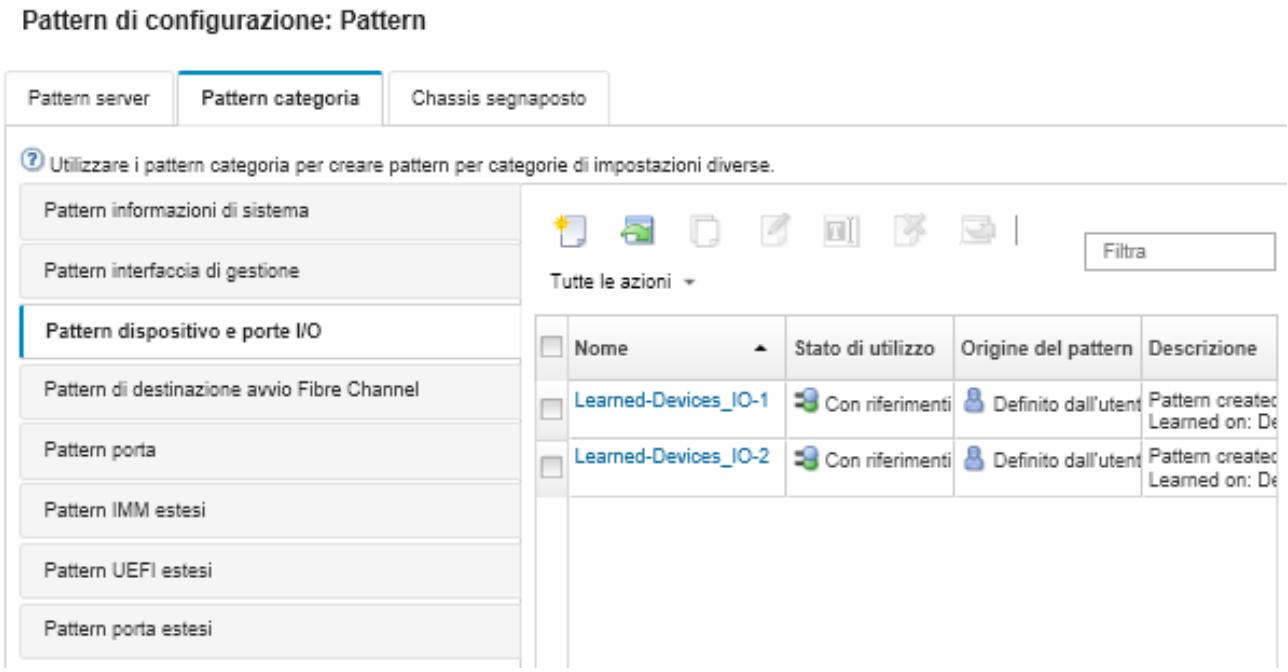
- Immettere un nome e una descrizione il pattern.
- Scegliere se abilitare o disabilitare il reindirizzamento della console. Se si abilita il reindirizzamento della console, è possibile scegliere di abilitare o disabilitare le seguenti opzioni:
  - **SOL (Serial Over LAN)**.

  - **Reindirizzamento processore di servizio**. Se si abilita il reindirizzamento del processore di servizio, è possibile scegliere di utilizzare la porta COM 1 o 2 per la porta seriale dei dati facoltativa legacy. Nota: se l'opzione è disabilitata, viene utilizzata sempre la porta COM 1.É possibile anche scegliere una delle seguenti modalità CLI:
    - Disabilita
    - Abilita con sequenza di tasti definita dall'utente
    - Abilita con sequenza di tasti compatibile con EMS
- Scegliere se abilitare o disabilitare le porte COM 1 e 2. Se si decide di abilitare le porte COM, specificare le seguenti impostazioni:
  - Velocità baud
  - Bit di dati
  - Parità
  - Bit di arresto
  - Emulazione testo
  - Attivo dopo avvio
  - Controllo flusso

Passo 5. Fare clic su **Crea**.

Risultati

Il nuovo pattern verrà elencato nella scheda **Pattern dispositivi e porte I/O** alla pagina Pattern di configurazione: pattern categoria:



Da questa pagina, è anche possibile eseguire le seguenti azioni su un pattern categoria selezionato:

- Modificare le impostazioni del pattern corrente facendo clic sull'icona **Modifica** ( ).
- Copiare un pattern esistente facendo clic sull'icona **Copia** ( ).
- Eliminare un pattern facendo clic sull'icona **Elimina** ( ).
- Rinominare un pattern facendo clic sull'icona **Rinomina** ( ).
- Importare o esportare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Definizione delle impostazioni di destinazione avvio Fibre Channel

È possibile configurare il server per l'avvio da un dispositivo SAN (Storage Area Network) invece che dall'unità disco locale creando un pattern di destinazione avvio Fibre Channel.

Procedura

Per creare un pattern di destinazione avvio Fibre Channel, completare i seguenti passaggi.

Limitazione: le destinazioni avvio Fibre Channel sono supportate solo dai nodi di elaborazione Flex. Non sono supportati i server rack e tower autonomi.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern categoria**.

Passo 3. Fare clic sulla linguetta laterale **Pattern di destinazione avvio Fibre Channel**, quindi sull'icona **Crea** ( ).

Passo 4. Nella finestra di dialogo Nuovo pattern di destinazione avvio Fibre Channel, specificare le seguenti informazioni.

- Immettere un nome e una descrizione il pattern.
- Specificare uno o più indirizzi WWPN e gli identificativi LUN da utilizzare come destinazioni avvio primarie. Inoltre, è possibile specificare facoltativamente uno o più indirizzi WWPN e gli identificativi LUN da utilizzare come destinazioni avvio secondarie.

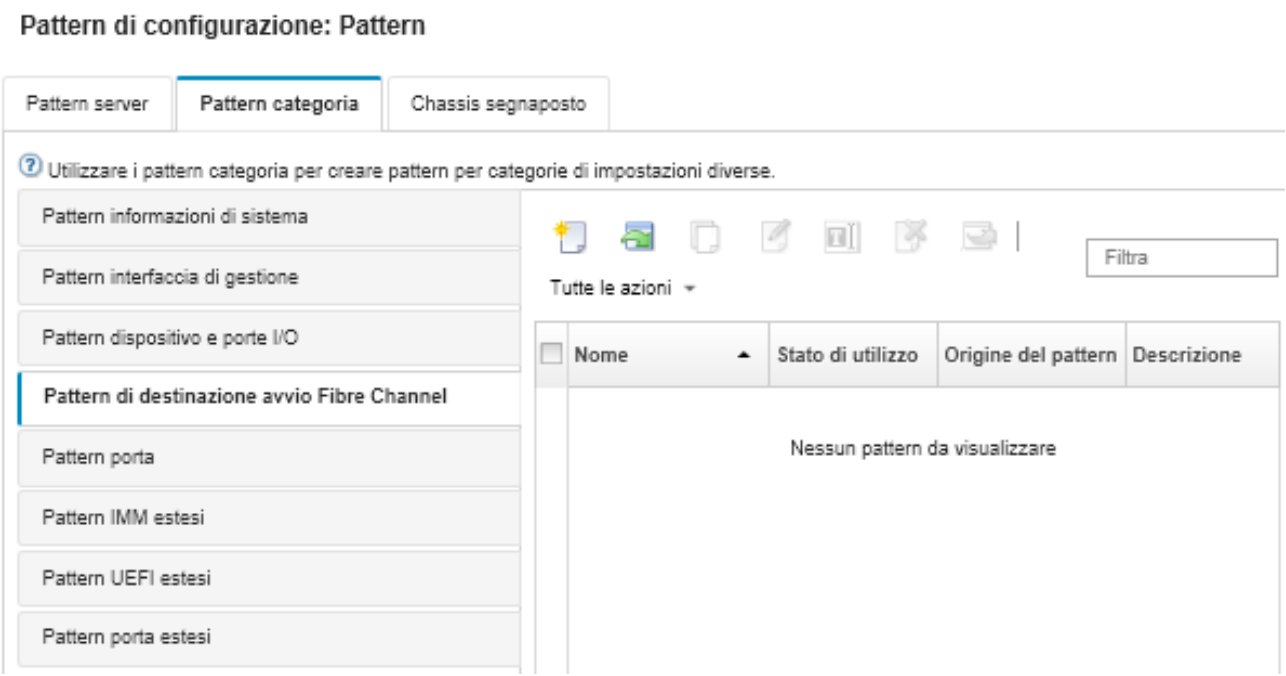
  Ad esempio, è possibile aggiungere i percorsi di storage primari come destinazioni primarie e i percorsi di storage secondari come destinazioni secondarie. Utilizzando gruppi di destinazione diversi in pattern server differenti, è possibile bilanciare il carico di storage durante le richieste di avvio simultanee da più host.

  Suggerimento: se si specifica `00:00:00:00:00:00:00:00` per WWPN, XClarity Administrator provare ad eseguire l'avvio dalla prima destinazione rilevata.

Passo 5. Fare clic su **Crea**.

Risultati

Il nuovo pattern verrà elencato nella scheda **Pattern di destinazione avvio Fibre Channel** nella pagina Pattern di configurazione: pattern categoria:



Da questa pagina, è anche possibile eseguire le seguenti azioni su un pattern categoria selezionato:

- Modificare le impostazioni del pattern corrente facendo clic sull'icona **Modifica** ( ).
- Copiare un pattern esistente facendo clic sull'icona **Copia** ( ).
- Eliminare un pattern facendo clic sull'icona **Elimina** ( ).
- Rinominare un pattern facendo clic sull'icona **Rinomina** ( ).
- Importare o esportare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Definizione delle impostazioni delle porte

È possibile definire le impostazioni tipiche delle porte di uno specifico adattatore I/O creando un pattern porte.

Informazioni su questa attività

È possibile utilizzare le impostazioni di rete dei pattern porta per configurare le porte interne dello switch. Tuttavia, non è possibile utilizzare i pattern porta per configurare le impostazioni globali degli switch, come ID VLAN, modalità UFP globale, modalità CEE globale e FIP globali. È necessario configurare manualmente le impostazioni globali utilizzando le seguenti regole compatibili con le impostazioni delle porte interne che si intende distribuire prima di distribuiate i pattern porta. Inoltre, non è possibile utilizzare i pattern porta per configurare l'etichettatura PVID. Consultare la documentazione fornita con lo switch per determinare i controlli di compatibilità tra le impostazioni globali e le impostazioni delle porte interne e scoprire come configurare le impostazioni dello switch.

- Quando PFC è configurato, verificare che **globalCEEState** sia impostato su "Attivato".
- Verificare che **globalCEEState** sia impostato su "Attivato" quando vport è impostato sulla modalità "FCoE".
- Quando l'opzione FIP è configurata, verificare che **globalCEEState** sia impostato su "Attivato" e che **globalFIPsState** sia impostato su "Attivato".
- Verificare che **globalUFPMode** sia impostato su "Abilita" quando la modalità della porta interna dello switch è impostata in modalità "UFP".

- Verificare che l'ID VLAN sia stato creato prima di aggiungere una porta a una rete VLAN specifica.

Procedura

Per creare un pattern porte adattatore I/O, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern categoria**.

Passo 3. Fare clic sulla linguetta laterale **Pattern porte**, quindi fare clic sull'icona **Crea** ( ).

Suggerimento: è anche possibile creare un nuovo pattern porta dalla pagina Aggiungi adattatore I/O facendo clic sull'icona **Crea** ( ) accanto alla selezione **Pattern porta iniziale**.

Passo 4. Nella finestra di dialogo Nuovo pattern porta, specificare le seguenti informazioni.

- Immettere un nome e una descrizione il pattern.
- Specificare le seguenti impostazioni di adattatore e compatibilità delle porte. Quando si assegnano dei pattern ad adattatori e porte, le impostazioni dei pattern vengono filtrate in base alla compatibilità con la porta o l'adattatore di destinazione.
  - Tipo di adattatore di destinazione
  - Modalità operativa della porta di destinazione, come:
    - Modalità pNIC
    - Modalità Virtual Fabric vNIC
    - Modalità indipendente switch vNIC
    - Modalità protocollo Unified Fabric vNIC

    Queste impostazioni abilitano la virtualizzazione NIC. Per ulteriori informazioni, vedere Virtualizzazione NIC nelle soluzioni Flex System Fabric.
  - Protocolli della porta di destinazione, come:
    - Solo Ethernet
    - Ethernet e FCoE
    - Ethernet e iSCSI
  - Pattern impostazioni estese porte, utilizzato per configurare le impostazioni aggiuntive delle porte ricavate dal server
- Se si imposta la modalità operativa della porta di destinazione su **modalità pNIC**, scegliere di applicare le impostazioni corrispondenti alle porte interne dello switch Flex, se applicabili. Se selezionato, è possibile configurare la rete VLAN aggiuntiva e le impostazioni avanzate:
  - Specificare il protocollo della porta di destinazione.
  - Se si imposta il protocollo della porta di destinazione su **Ethernet e FCoE**, selezionare e specificare facoltativamente l'ID priorità 2.
- Se si imposta la modalità operativa della porta di destinazione su **Modalità Virtual Fabric vNIC**, configurate le impostazioni della funzione fisica, come il tipo e l'etichetta VLAN di ogni funzione.
- Se si imposta la modalità operativa della porta di destinazione su **Modalità indipendente switch vNIC**, specificare il tipo, la larghezza di banda minima e l'etichetta VLAN di ciascuna funzione abilitata. È inoltre possibile scegliere di applicare le impostazioni corrispondenti alle porte interne dello switch Flex, dove possibile. Se selezionato, è possibile configurare la porta interna aggiuntiva dello switch e le impostazioni avanzate:
  - Specificare la rete LAN predefinita, utilizzata solo dal sistema operativo per inviare i pacchetti senza etichetta.
  - Specificare un elenco separato da virgola di reti VLAN.
  - Scegliere di configurare il controllo manuale e specificare i trigger.

  - Scegliere di configurare il tipo di controllo del flusso, come
    - Mantieni controllo flusso esistente
    - Controllo flusso basato su priorità
    - Controllo flusso a livello di collegamento

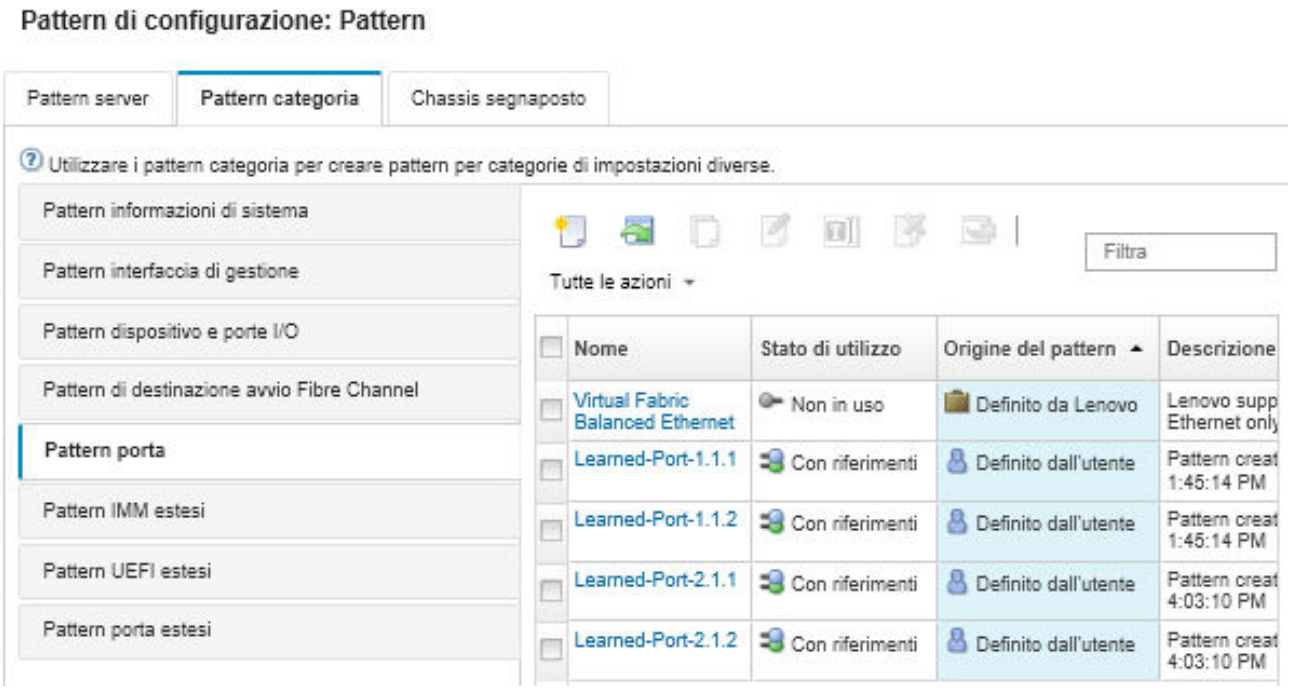
    Per ulteriori informazioni sui tipi di controllo del flusso, consultare la documentazione fornita con lo switch Flex.
- Se si imposta la modalità operativa della porta di destinazione su **Modalità protocollo Unified Fabric vNIC**, scegliere di applicare le impostazioni corrispondenti alle porte interne dello switch Flex, se applicabili. Se selezionato, è possibile configurare la funzione UFP aggiuntiva e le impostazioni avanzate:
  - Specificare la modalità QoS (larghezza di banda o priorità).
  - Scegliere di abilitare l'etichettatura VLAN ID predefinita e specificare modalità, larghezza di banda minima ed etichetta VLAN per ciascuna funzione abilitata.
  - Scegliere di configurare l'errore di livello 2 e specificare il numero di trigger per ogni funzione.
  - Per la modalità QoS della larghezza di banda, specificare il tipo di controllo del flusso (basato su priorità, livello di collegamento o controllo del flusso esistente).
  - Per la modalità QoS della larghezza di banda, scegliere se abilitare la priorità 4 quando iSCSI è selezionato.

  Nota: Quando si definiscono i trigger di failover, verificare che l'opzione di failover globale sia impostata su "Attivato".

Passo 5. Fare clic su **Crea**.

Risultati

Il nuovo pattern verrà elencato nella scheda **Pattern porta** della pagina Pattern di configurazione: pattern categoria:



Da questa pagina, è anche possibile eseguire le seguenti azioni su un pattern categoria selezionato:

- Modificare le impostazioni del pattern corrente facendo clic sull'icona **Modifica** ( ).
- Copiare un pattern esistente facendo clic sull'icona **Copia** ( ).

- Eliminare un pattern facendo clic sull'icona **Elimina** ().
- Rinominare un pattern facendo clic sull'icona **Rinomina** ().
- Importare o esportare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Definizione delle impostazioni di controller di gestione esteso

Le impostazioni del controller di gestione della scheda di base vengono ricavate e create dinamicamente da uno specifico server gestito. Lenovo XClarity Administrator crea questi pattern contestualmente alla creazione di un pattern server da un server esistente. Non è possibile creare manualmente pattern di controller di gestione esteso, ma è possibile copiare e modificare i pattern già creati.

Prima di iniziare

Nota: L'impostazione termica del modulo IMM potrebbe essere in conflitto con l'impostazione della modalità operativa UEFI. In questo caso, le impostazioni UEFI sovrascrivono l'impostazione del modulo IMM quando il dispositivo viene riavviato e tutte le impostazioni termiche definite in un pattern esteso del controller di gestione della scheda di base non saranno conformi. Per risolvere il problema di mancata conformità, rimuovere l'impostazione dal pattern esteso del controller di gestione della scheda di base oppure selezionare un'impostazione che non entri in conflitto con l'impostazione della modalità operativa UEFI corrente.

Procedura

Per modificare i pattern di controller di gestione esteso, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern categoria**.

Passo 3. Fare clic sulla linguetta laterale **Pattern BMC estesi**.

Passo 4. Selezionare il pattern da modificare e fare clic sull'icona **Modifica** ().

Passo 5. Modificare i campi appropriati.

Per selezionare le impostazioni che si desidera includere nel pattern categoria, fare clic sulle impostazioni **Includi/Escludi**.

- Per configurare le impostazioni DNS, fare clic su **Interfaccia impostazioni di rete → Configurazione DNS**. È possibile abilitare l'opzione DNS, selezionare il protocollo IP e specificare fino a tre indirizzi IPv4 o IPv6 e abilitare il rilevamento degli indirizzi IP di XClarity Administrator.

  Nota: Per i dispositivi Flex System, è possibile configurare solo l'indirizzo IP da utilizzare per rilevare il server XClarity Administrator.

- Per configurare le impostazioni NTP, fare clic su **Interfaccia impostazioni di rete → Impostazione NTP modulo integrato**. È possibile specificare il nome host e la frequenza per un massimo di 4 server NTP.

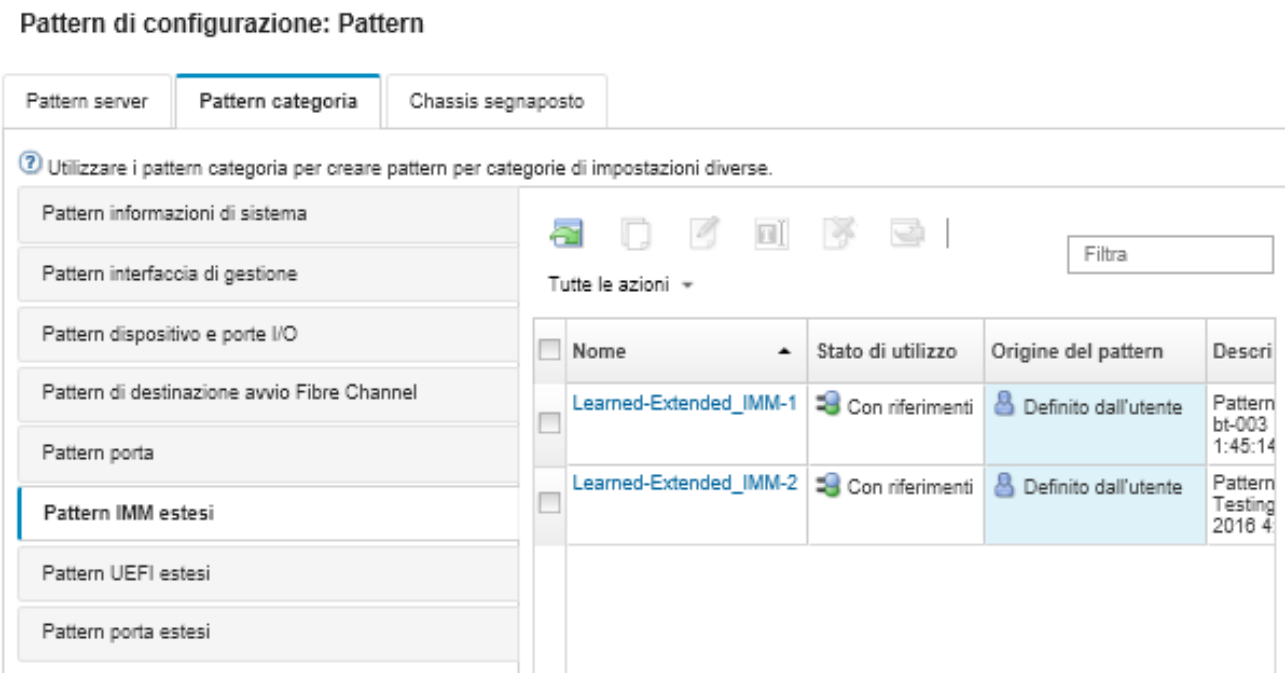
  Nota: Per i dispositivi Flex System, non è possibile configurare le impostazioni NTP.

- (Solo server rack) Per le impostazioni di data e ora, fare clic su **Impostazioni generali → Impostazioni orologio modulo integrato**. È possibile specificare il fuso orario (offset UTC), abilitare o disabilitare l'ora legale (DST) e scegliere se utilizzare l'ora UTC o l'ora locale sull'host.
- Per modificare le impostazioni di sicurezza dell'account utente, fare clic su **Configurazione sicurezza account**

Passo 6. Fare clic su **Salva** per salvare le modifiche al pattern categoria corrente oppure fare clic su **Salva con nome** per salvare le modifiche in un nuovo pattern categoria.

Risultati

Il pattern categoria modificato viene elencato nella scheda **Pattern BMC estesi** della pagina Pattern di configurazione: pattern categoria:



Da questa pagina, è anche possibile eseguire le seguenti azioni su un pattern categoria selezionato:

- Copiare un pattern esistente facendo clic sull'icona **Copia** ( ).
- Eliminare un pattern facendo clic sull'icona **Elimina** ( ).
- Rinominare un pattern facendo clic sull'icona **Rinomina** ( ).
- Importare o esportare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Definizione delle impostazioni UEFI estese

Le impostazioni UEFI (Unified Extensible Firmware Interface) estesa vengono ricavate e create dinamicamente da uno specifico server gestito. Lenovo XClarity Administrator crea questi pattern contestualmente alla creazione di un pattern server da un server esistente. Non è possibile creare manualmente pattern UEFI estesa, ma è possibile copiare e modificare i pattern già creati.

Informazioni su questa attività

I seguenti pattern UEFI estesi vengono predefiniti da Lenovo XClarity Administrator per ottimizzare i server per ambienti specifici.

- **Opzioni di installazione ESXi**
- **Efficienza - Prestazioni preferite**
- **Efficienza - Alimentazione preferita**
- **Prestazioni massime**
- **Alimentazione minima**

Nota:

- la modifica delle impostazioni di sicurezza UEFI (tra cui la configurazione di criteri di presenza fisica, avvio sicuro e TPM (Trusted Platform Module)) non è supportata mediante pattern UEFI estesa.

- È possibile modificare la password di amministratore UEFI per i server ThinkSystem e ThinkAgile selezionati dalla pagina Server facendo clic su **Tutte le azioni → Sicurezza → Password amministratore UEFI**. È richiesto il livello firmware 20A di Lenovo XClarity Controller.

Procedura

Per modificare i pattern UEFI estesa, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern categoria**.

Passo 3. Fare clic sulla linguetta laterale **Pattern UEFI estesi**.

Passo 4. Selezionare il pattern da modificare e fare clic sull'icona **Modifica** ( ).

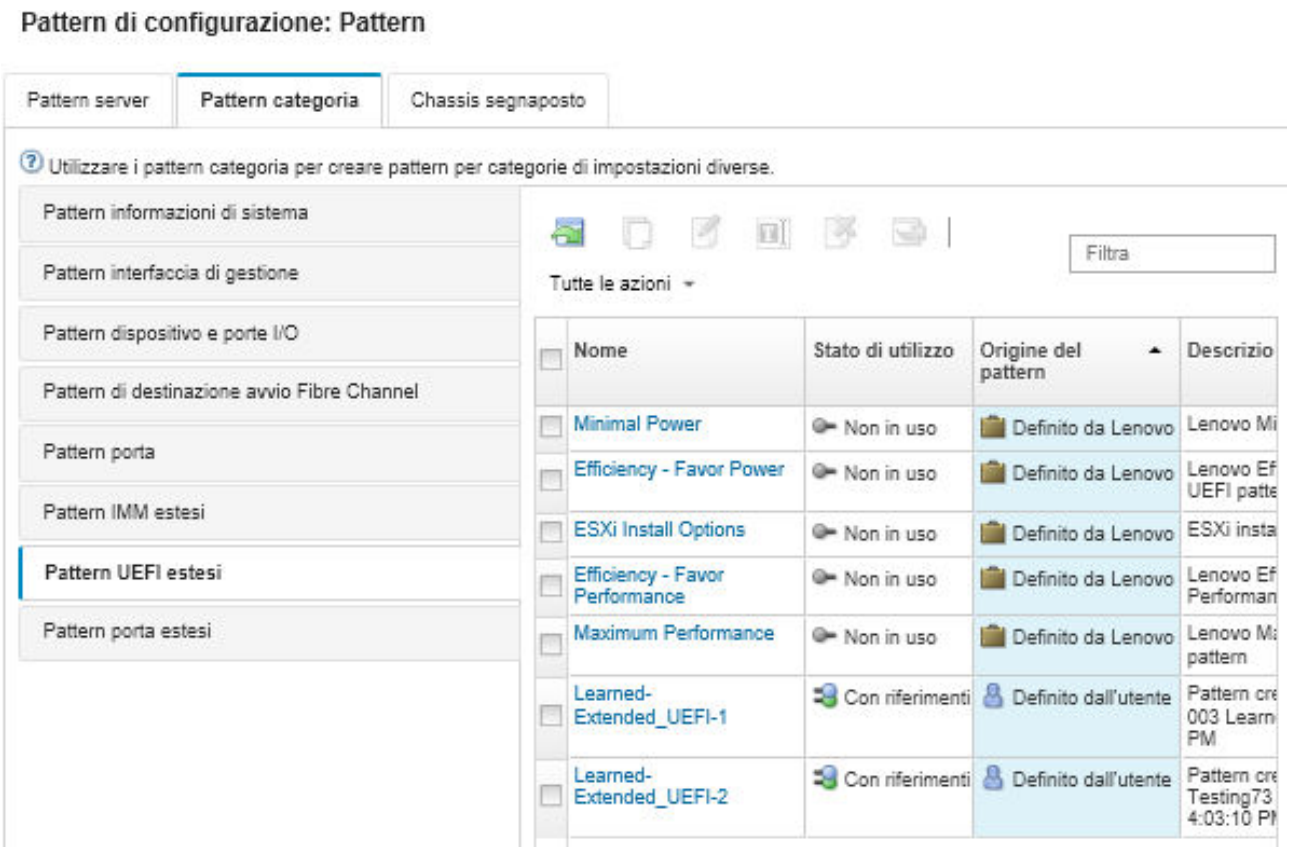
Passo 5. Modificare i campi appropriati.

Per selezionare le impostazioni che si desidera includere nel pattern categoria, fare clic sulle impostazioni **Includi/Escludi**.

Passo 6. Fare clic su **Salva** per salvare le modifiche al pattern categoria corrente oppure fare clic su **Salva con nome** per salvare le modifiche in un nuovo pattern categoria.

Risultati

Il pattern categoria modificato è elencato nella scheda **Pattern UEFI estesi** nella pagina Pattern di configurazione: pattern categoria:



Da questa pagina, è anche possibile eseguire le seguenti azioni su un pattern categoria selezionato:

- Copiare un pattern esistente facendo clic sull'icona **Copia** ().
- Eliminare un pattern facendo clic sull'icona **Elimina** ().
- Rinominare un pattern facendo clic sull'icona **Rinomina** ().
- Importare o esportare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Definizione delle impostazioni della porta estesa

Le impostazioni di porta estesa vengono ricavate e create dinamicamente da uno specifico server gestito. Lenovo XClarity Administrator crea questi pattern contestualmente alla creazione di un pattern server da un server esistente. Non è possibile creare manualmente pattern di porta estesa, ma è possibile copiare e modificare i pattern già creati.

Informazioni su questa attività

XClarity Administrator fornisce i seguenti pattern di porta estesa predefiniti:

- **Ethernet bilanciata Virtual Fabric**. Pattern di porta fornito da Lenovo per la modalità Virtual Fabric vNIC, solo Ethernet

Alcune impostazioni a livello di dispositivo sugli adattatori I/O Mellanox e Broadcom devono presentare lo stesso valore su tutte le porte. Se le impostazioni presentano valori diversi su porte diverse, verranno utilizzate le impostazioni per un'unica porta e le impostazioni per altre porte non saranno conformi. Per risolvere il problema di non conformità, selezionare lo stesso valore per le impostazioni a livello di dispositivo.

Per gli adattatori I/O Mellanox, è necessario configurare le seguenti impostazioni sullo stesso valore su tutte le porte.
- Impostazioni energetiche avanzate
- Funzioni virtuali PCI pubblicizzate
- Limitatore di alimentazione dello slot
- Modalità di virtualizzazione

Per gli adattatori I/O Broadcom, è necessario configurare le seguenti impostazioni sullo stesso valore su tutte le porte.
- Timeout messaggio banner
- Limite BW
- Limite BW valido
- Prenotazione BW
- Prenotazione BW valida
- Abilitazione della funzionalità PME
- Numero massimo di vettori PF MSI-X
- Modalità multifunzione
- Numero di vettori MSI-X per VF
- Numero di VF per PF
- ROM opzionale
- SR-IOV
- Supporto RDMA

Procedura

Per modificare i pattern di porta estesa, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern categoria**.

Passo 3. Fare clic sulla linguetta laterale **Pattern porta estesi**.

Passo 4. Selezionare il pattern da modificare e fare clic sull'icona **Modifica** ( ).

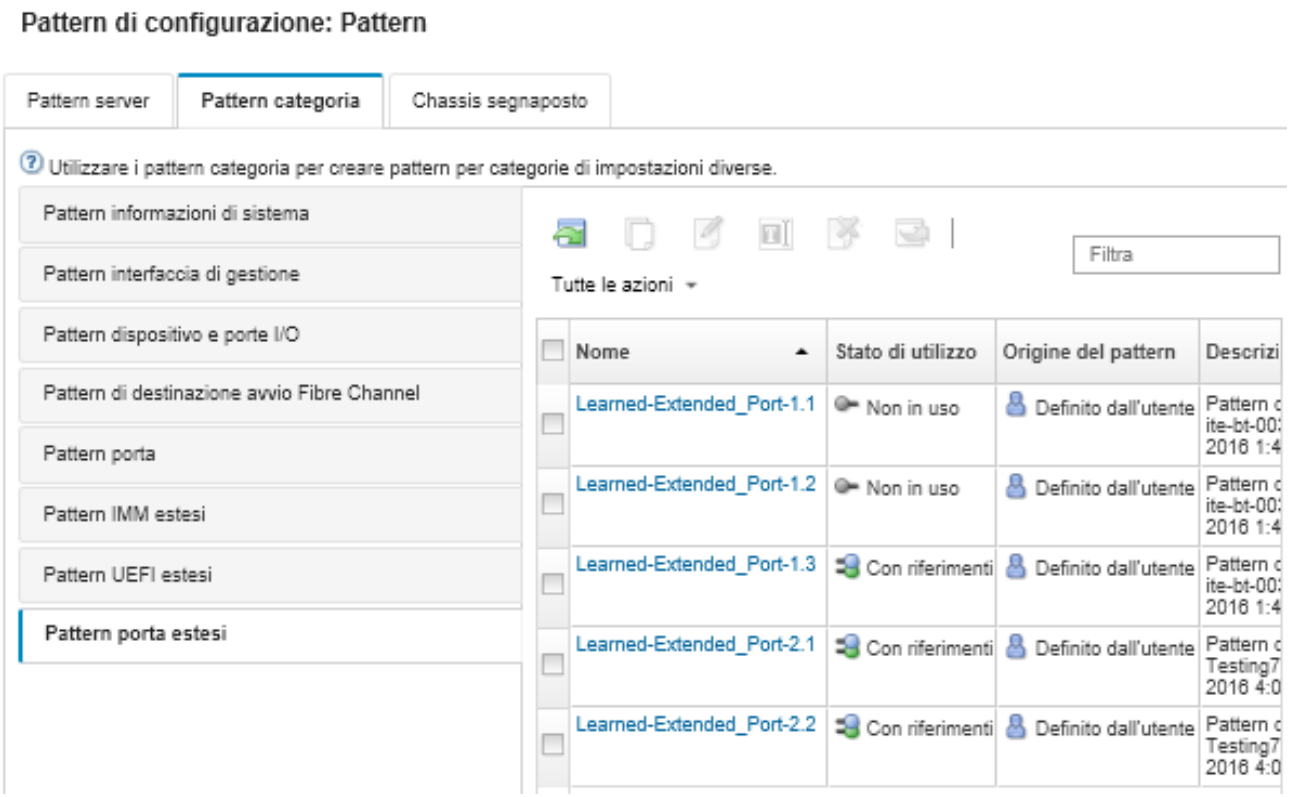
Passo 5. Modificare i campi appropriati.

Per selezionare le impostazioni che si desidera includere nel pattern categoria, fare clic sulle impostazioni **Includi/Escludi**.

Passo 6. Fare clic su **Salva** per salvare le modifiche al pattern categoria corrente oppure fare clic su **Salva con nome** per salvare le modifiche in un nuovo pattern categoria.

Risultati

Il pattern categoria modificato viene elencato nella scheda **Pattern porta estesi** della pagina Pattern di configurazione: pattern categoria:



Da questa pagina, è anche possibile eseguire le seguenti azioni su un pattern categoria selezionato:

- Copiare un pattern esistente facendo clic sull'icona **Copia** ( ).
- Eliminare un pattern facendo clic sull'icona **Elimina** ( ).
- Rinominare un pattern facendo clic sull'icona **Rinomina** ( ).
- Importare o esportare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Definizione delle impostazioni BIOS SR635/SR655 estese

Le impostazioni BIOS SR635/SR655 estese vengono ricavate e create dinamicamente da uno specifico server gestito. Lenovo XClarity Administrator crea questi pattern quando si genera un pattern server da un server ThinkSystem SR635 o SR655 esistente. Non è possibile creare manualmente pattern BIOS SR635/SR655 estesi, ma è possibile copiare e modificare i pattern già creati.

Procedura

Per modificare i pattern BIOS SR635/SR655 estesi, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern categoria**.

Passo 3. Fare clic sulla linguetta laterale **Pattern BIOS SR635/SR655 estesi**.

Passo 4. Selezionare il pattern da modificare e fare clic sull'icona **Modifica** ().

Passo 5. Modificare i campi appropriati.

Per selezionare le impostazioni che si desidera includere nel pattern categoria, fare clic sulle impostazioni **Includi/Escludi**.

Passo 6. Fare clic su **Salva** per salvare le modifiche al pattern categoria corrente oppure fare clic su **Salva con nome** per salvare le modifiche in un nuovo pattern categoria.

Risultati

Il pattern categoria modificato viene elencato nella scheda **Pattern BIOS SR635/SR655 estesi** della pagina Pattern di configurazione: pattern categoria:

Da questa pagina, è anche possibile eseguire le seguenti azioni su un pattern categoria selezionato:

- Copiare un pattern esistente facendo clic sull'icona **Copia** ().
- Eliminare un pattern facendo clic sull'icona **Elimina** ().
- Rinominare un pattern facendo clic sull'icona **Rinomina** ().
- Importare o esportare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Definizione delle impostazioni BIOS estese di ThinkServer CPlus

Le impostazioni estese del BIOS di ThinkServer CPlus vengono ricavate e create dinamicamente da uno specifico server gestito. Lenovo XClarity Administrator crea questi pattern quando si genera un pattern server da un server ThinkServer CPlus esistente. Non è possibile creare manualmente pattern estesi del BIOS di ThinkServer CPlus, ma è possibile copiare e modificare i pattern già creati.

Procedura

Per modificare i pattern estesi del BIOS di ThinkServer CPlus, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern categoria**.

Passo 3. Fare clic sulla linguetta laterale **Pattern BIOS ThinkServer CPlus esteso**.

Passo 4. Selezionare il pattern da modificare e fare clic sull'icona **Modifica** ().

Passo 5. Modificare i campi appropriati.

Per selezionare le impostazioni che si desidera includere nel pattern categoria, fare clic sulle impostazioni **Includi/Escludi**.

Passo 6. Fare clic su **Salva** per salvare le modifiche al pattern categoria corrente oppure fare clic su **Salva con nome** per salvare le modifiche in un nuovo pattern categoria.

Risultati

Il pattern categoria modificato viene elencato nella scheda **Pattern BIOS ThinkServer CPlus esteso** nella pagina Pattern di configurazione: pattern categoria:

Da questa pagina, è anche possibile eseguire le seguenti azioni su un pattern categoria selezionato:

- Copiare un pattern esistente facendo clic sull'icona **Copia** ().
- Eliminare un pattern facendo clic sull'icona **Elimina** ().
- Rinominare un pattern facendo clic sull'icona **Rinomina** ().
- Importare o esportare i pattern server (vedere Esportazione e importazione di pattern server e categoria).

Distribuzione di un pattern server in un server

È possibile distribuire un pattern server in uno o più server gestiti. È inoltre possibile distribuire un pattern server in uno o più vani vuoti in uno chassis gestito da Lenovo XClarity Administrator o in uno chassis segnaposto. La distribuzione di un pattern server prima dell'installazione del server riserva gli indirizzi IP di gestione e gli indirizzi Ethernet o Fibre Channel virtuali ed effettua il push dell'impostazione di rete nelle relative porte interne dello switch.

Prima di iniziare

Leggere le considerazioni sulla configurazione del server prima di tentare di applicare un pattern server ai dispositivi gestiti (vedere Distribuzione di un pattern server in un server).

Procedura

Per distribuire un pattern server in un server gestito, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern di configurazione server**. Viene visualizzata la pagina Pattern di configurazione server.

Passo 2. Fare clic sulla scheda **Pattern server**.

Passo 3. Selezionare il pattern server da distribuire e fare clic sull'icona **Distribuisci** ().

Verrà visualizza la finestra di dialogo Distribuisci pattern server con il pattern server selezionato elencato in **Pattern da distribuire**.

Passo 4. Scegliere quando attivare le configurazioni:

- **Completo**. Accende o riavvia immediatamente il server per attivare le configurazioni del server, del controller di gestione della scheda di base e dell'interfaccia UEFI (Unified Extensible Firmware Interface).
- **Parziale**. (predefinito) Attiva immediatamente le configurazioni del controller di gestione, ma posticipa l'attivazione delle configurazioni del server e dell'interfaccia UEFI al successivo riavvio del server. Per l'attivazione completa del profilo è necessario accendere o riavviare manualmente il server.

  Nota: Quando si distribuiscono i pattern server che includono solo le impostazioni IMM (incluse le informazioni di sistema, l'interfaccia di gestione e i pattern categoria BMC estesi), non è necessario riavviare il server.
- **Rinviato**. Genera un profilo per le configurazioni del server, del controller di gestione e dell'interfaccia UEFI, ma non attiva le impostazioni di configurazione nel server. Per l'attivazione completa del profilo, è necessario attivare manualmente quest'ultimo riavviando il server.

Nota: Subito dopo la distribuzione, le impostazioni di rete nelle relative porte interne dello switch verranno sottoposte al push nello switch, indipendentemente dalla configurazione di attivazione.

Passo 5. Scegliere uno o più server o vani vuoti dello chassis in cui si desidera distribuire il pattern server.

Nota: Per visualizzare un elenco di vani vuoti dello chassis, selezionare **Mostra vani vuoti**.

Passo 6. Fare clic su **Distribuisci**. Verrà visualizzata una finestra di dialogo contenente lo stato di distribuzione di ciascun vano selezionato.

Passo 7. Fare nuovamente clic su **Distribuisci** per avviare il processo di distribuzione.

Nota: Il completamento della distribuzione potrebbe richiedere alcuni minuti. Durante la distribuzione, un profilo del server viene creato e assegnato a ciascun server o vano dello chassis selezionato.

Passo 8. Fare clic su **Chiudi**.

Al termine

Per monitorare l'avanzamento della distribuzione, fare clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator. È inoltre possibile monitorare la creazione dei profili del server facendo clic su **Provisioning → Profili server**. Al termine della distribuzione, esaminare i profili del server generati e registrare l'indirizzo IP di gestione ed eventuali indirizzi Ethernet o Fibre Channel virtualizzati.

Se si è distribuito un pattern server in un server esistente e si è selezionata l'attivazione:

- **Completo**, verrà creato un profilo per ciascun server, la configurazione verrà propagata a ognuno di essi e ciascun server verrà riavviato per attivare le modifiche di configurazione.
- **Parziale**, verrà creato un profilo per ciascun server e la configurazione verrà propagata a ognuno di essi. Per l'attivazione completa delle modifiche di configurazione, è necessario accendere o riavviare manualmente ciascun server (vedere Accensione e spegnimento di un server).
- **Rinviato**, verrà creato un profilo per ciascun server. È necessario attivare manualmente il profilo nel server (vedere Attivazione di un profilo del server).

Se si è distribuito un pattern server in un vano vuoto in uno chassis gestito o uno chassis segnaposto, una volta che i nodi di elaborazione saranno stati fisicamente installati nei vani dello chassis appropriati, quindi rilevati e gestiti da Lenovo XClarity Administrator, sarà necessario distribuire e attivare il profilo del server nei nodi di elaborazione appena installati (vedere Attivazione di un profilo del server).

Se uno o più server non si avviano in seguito alla distribuzione di un nuovo pattern server, il problema potrebbe essere riconducibile al fatto che le impostazioni di avvio sono state sovrascritte dalle impostazioni di avvio predefinite nel pattern server. Per i sistemi operativi installati in modalità UEFI, il ripristino delle impostazioni predefinite potrebbe richiedere ulteriori passaggi per ripristinare la configurazione di avvio. Per esempi sul ripristino delle impostazioni di avvio nei server che eseguono Windows o su Linux, vedere Ripristino delle impostazioni di avvio in seguito alla distribuzione di pattern server.

Modifica di un pattern server

È possibile apportare successive modifiche di configurazione a un pattern server esistente. Se il pattern server originale viene distribuito ai server (se è in uso), è possibile ridistribuire il pattern server modificato a tutti i server o a un insieme secondario di questi server.

Informazioni su questa attività

Nota: Se si sceglie di non distribuire il pattern server modificato a un insieme di server, questi server restano associati al pattern server originale non modificato.

Modificando il pattern server, è possibile controllare una configurazione comune da un'unica posizione e conservare la serie originale di assegnazioni degli indirizzi virtuali.

Procedura

Per modificare un pattern server, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern di configurazione server**. Viene visualizzata la pagina Pattern di configurazione server.

Passo 2. Fare clic sulla scheda **Pattern server**.

Passo 3. Selezionare il pattern server da modificare e fare clic sull'icona **Modifica** (). Verrà visualizzata la finestra di dialogo Modifica guidata pattern server.

Passo 4. Immettere il nome del pattern e una descrizione.

Passo 5. Scegliere la configurazione di storage locale da applicare quando il pattern viene distribuito a un server e fare clic su **Avanti**.

Per ulteriori informazioni sulle impostazioni dello storage locale, vedere Definizione di storage locale.

Passo 6. **Facoltativo:** modificare l'indirizzamento dell'adattatore I/O e definire gli adattatori I/O aggiuntivi in modo che corrispondano alla configurazione hardware prevista per questo pattern e fare clic su **Avanti**.

Per informazioni sulle impostazioni dell'adattatore I/O, vedere Definizione degli adattatori I/O.

Passo 7. Definire l'ordine di avvio da applicare quando questo pattern viene distribuito a un server e fare clic su **Avanti**.

Per informazioni sulle impostazioni delle destinazioni avvio SAN, vedere Definizione delle opzioni di avvio.

Passo 8. Selezionare le impostazioni firmware dall'elenco di pattern categoria esistenti.

Per creare nuovi pattern categoria, fare clic sull'icona **Crea** ().

Per informazioni sulle impostazioni firmware, vedere Definizione delle impostazioni firmware.

Passo 9. Fare clic su **Salva** per salvare le modifiche di configurazione nel pattern server corrente oppure su **Salva con nome** per salvare le modifiche di configurazione in un nuovo pattern server.

Passo 10. Scegliere di salvare le modifiche nel pattern server corrente o in un nuovo pattern server.

- Fare clic su **Salva** per salvare le modifiche nel pattern server corrente. Dalla finestra di dialogo "Salva e ridistribuisci pattern", completare le seguenti operazioni:
  1. Scegliere quando attivare le configurazioni.
     - **Completo**. Accende o riavvia immediatamente il server per attivare le configurazioni del server, del controller di gestione della scheda di base e dell'interfaccia UEFI (Unified Extensible Firmware Interface).
     - **Parziale**. (predefinito) Attiva immediatamente le configurazioni del controller di gestione, ma posticipa l'attivazione delle configurazioni del server e dell'interfaccia UEFI al successivo riavvio del server. Per l'attivazione completa del profilo è necessario accendere o riavviare manualmente il server.

       Nota: Quando si distribuiscono i pattern server che includono solo le impostazioni IMM (incluse le informazioni di sistema, l'interfaccia di gestione e i pattern categoria BMC estesi), non è necessario riavviare il server.

  Nota: Subito dopo la distribuzione, le impostazioni di rete nelle relative porte interne dello switch verranno sottoposte al push nello switch, indipendentemente dalla configurazione di attivazione.

2. Selezionare i server di destinazione in cui si desidera ridistribuire le modifiche della configurazione. È possibile scegliere tutti i server in cui è stato distribuito il pattern server originale o un sottoinsieme di questi server.
3. Fare clic su **Ridistribuisci**

- Fare clic su **Salva con nome** per salvare le modifiche in un nuovo pattern server. Per distribuire il nuovo pattern, vedere Distribuzione di un pattern server in un server.

Esportazione e importazione di pattern server e categoria

In presenza di più istanze di Lenovo XClarity Administrator, è possibile esportare i pattern server e categoria da un'istanza di XClarity Administrator e includerli in un'altra istanza di XClarity Administrator.

Informazioni su questa attività

È possibile esportare solo pattern server e categoria. Non è possibile esportare criteri, pool di indirizzi e profili. Per i pattern esportati verrà annullata l'associazione a eventuali pool di indirizzi di riferimento. Per utilizzare i pool di indirizzi in un pattern importato, modificarlo e riassociarlo ai pool in XClarity Administrator in cui sono importati.

Nota: Quando si esporta un pattern server, vengono esportati anche i pattern categoria associati.

Procedura

- Per esportare uno o più pattern:
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Pattern di configurazione server**. Viene visualizzata la pagina Pattern di configurazione server.
  2. Fare clic sulla scheda **Pattern server** o **Pattern categoria**.
  3. Selezionare uno o più pattern da esportare.
  4. Fare clic sull'icona **Esporta** ().
  5. Fare clic su **Esporta** per esportare i pattern.
  6. Salvare il file di dati pattern nel sistema locale.

     Nota: Se un pattern esportato fa riferimento a pool di indirizzi, questi riferimenti verranno rimossi dal pattern esportato al fine di evitare i conflitti in fase di importazione del pattern in un'altra istanza di XClarity Administrator. Una volta reimportato il pattern, sarà possibile modificarlo e assegnare i pool di indirizzi desiderati.
- Per importare uno o più pattern:
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Pattern di configurazione server**. Viene visualizzata la pagina Pattern di configurazione server.
  2. Fare clic sull'icona **Importa** () per importare i pattern. Verrà visualizzata la finestra di dialogo Importa pattern.
  3. Fare clic su **Seleziona file** e selezionare un file di dati pattern da importare. Ripetere l'operazione per altri file di dati pattern.
  4. Fare clic su **Importa** per importare i file selezionati.

     Verrà visualizzato un report di riepilogo con un elenco dei pattern importati, dei pattern rinominati per evitare conflitti di denominazione e dei pattern ignorati poiché già esistenti.

Utilizzo di profili del server

Un *profilo del server* è un'istanza di un pattern server applicato a un server specifico. Quando un pattern server viene distribuito in uno o più server, verranno automaticamente generati e assegnati profili del server. Viene creato un profilo del server per ogni server di destinazione. Ciascun profilo del server contiene la configurazione specifica per un singolo server e contiene informazioni (tra cui nome assegnato, indirizzi IP e indirizzi MAC) univoche per tale server.

Informazioni su questa attività

Il profilo del server viene attivato durante il processo di avvio del controller di gestione della scheda di base. È possibile scegliere di:

- riavviare il server quando il pattern viene distribuito per attivare immediatamente il profilo
- rinviare l'attivazione fino al riavvio successivo
- rinviare l'attivazione fino all'attivazione manuale del profilo del server.

Da un singolo pattern server è possibile ereditare più profili di server. Una volta distribuito un pattern in uno o più server, sarà possibile distribuire rapidamente le modifiche di configurazione a più server modificando il pattern server e i pattern categoria principali. I profili dipendenti verranno automaticamente aggiornati e ridistribuiti nei server associati. Modificando il pattern server, è possibile controllare una configurazione comune da un'unica posizione.

Se si sostituisce un server esistente o si installa un server sottoposto a preprovisioning in un vano vuoto di uno chassis, sarà necessario attivare il profilo per il nuovo server al fine di effettuare il provisioning delle modifiche di configurazione nel nuovo server.

Nota: È possibile distribuire un pattern server in più server, ma non è possibile distribuire più pattern in un singolo server.

È possibile modificare il profilo associato a un server in vari modi, seconda del motivo alla base della modifica.

- Se si desidera spostare o reimpiegare un server:
  1. Disattivare il profilo attuale sul server corrente (vedere Disattivazione di un profilo del server).
  2. Distribuire il nuovo pattern nel nuovo server (vedere Distribuzione di un pattern server in un server).
- Se un server è guasto e si desidera utilizzare un server di riserva:
  1. Disattivare il profilo attuale sul server guasto (vedere Disattivazione di un profilo del server).
  2. Attivare lo stesso profilo sul server di riserva (vedere Attivazione di un profilo del server).
  3. Una volta riparato il server guasto, sarà possibile ripetere questi passaggi per eseguire nuovamente lo switch del profilo.
- Se un server è guasto e si desidera sostituire l'hardware:
  1. Disattivare il profilo attuale sul server guasto (vedere Disattivazione di un profilo del server).
  2. Sostituire il server guasto.
  3. Attivare lo stesso profilo sul nuovo server (vedere Attivazione di un profilo del server).

Importante:

- Se si utilizza la virtualizzazione degli indirizzi, un server manterrà l'indirizzo MAC o WWN assegnato fino allo spegnimento. In caso di disattivazione di un profilo in cui è abilitata la virtualizzazione degli indirizzi, la casella di controllo **Spegni il server** è selezionata per impostazione predefinita. Accertarsi che il server originale venga spento prima di attivare il profilo inattivo in un altro server per evitare conflitti negli indirizzi.

- Se si elimina un profilo che non sia l'ultimo creato, gli indirizzi WWN e MAC virtuali *non* vengono rilasciati dal pool di indirizzi. Per ulteriori informazioni, vedere Eliminazione di un profilo del server.
- Le impostazioni di un server possono diventare non conformi al profilo del server, se le impostazioni vengono modificate senza utilizzare i pattern di configurazione o se si è verificato un problema durante la distribuzione, come un problema relativo a un firmware o a un'impostazione non valida. È possibile determinare lo stato della conformità di ciascun server dalla pagina "Pattern di configurazione: Profili server".

Attivazione di un profilo del server

È possibile attivare un profilo del server su un server sostituito, riassegnato, appena installato e gestito.

Informazioni su questa attività

Se si sostituisce un server esistente o si installa un server sottoposto a preprovisioning in un vano vuoto di uno chassis, sarà necessario attivare il profilo per il nuovo server al fine di effettuare il provisioning delle modifiche di configurazione nel nuovo server.

Importante:

- Se si utilizza la virtualizzazione degli indirizzi, un server manterrà l'indirizzo MAC o WWN assegnato fino allo spegnimento. In caso di disattivazione di un profilo in cui è abilitata la virtualizzazione degli indirizzi, la casella di controllo **Spegni il server** è selezionata per impostazione predefinita. Accertarsi che il server originale venga spento prima di attivare il profilo inattivo in un altro server per evitare conflitti negli indirizzi.
- Se si elimina un profilo che non sia l'ultimo creato, gli indirizzi WWN e MAC virtuali *non* vengono rilasciati dal pool di indirizzi. Per ulteriori informazioni, vedere Eliminazione di un profilo del server.
- Le impostazioni di un server possono diventare non conformi al profilo del server, se le impostazioni vengono modificate senza utilizzare i pattern di configurazione o se si è verificato un problema durante la distribuzione, come un problema relativo a un firmware o a un'impostazione non valida. È possibile determinare lo stato della conformità di ciascun server dalla pagina "Pattern di configurazione: Profili server".

Procedura

Per attivare un profilo del server, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Profili server**. Viene visualizzata la pagina Pattern di configurazione: Profili server.

Passo 2. Selezionare il profilo del server da attivare.

Suggerimento: lo stato corrente dei profili del server è elencato nella colonna **Stato profilo**. È possibile attivare il profilo del server con stato di attivazione "Inattivo" o "In sospeso".

Passo 3. Fare clic sull'icona **Attiva profilo server** ().

Passo 4. Fare clic su **Attiva**.

Se lo stato del profilo è: in sospeso, attivo o errore (attivo), è possibile scegliere quando attivare la distribuzione:

- **Completo**. Accende o riavvia immediatamente il server per attivare le configurazioni del server, del controller di gestione della scheda di base e dell'interfaccia UEFI (Unified Extensible Firmware Interface).
- **Parziale**. (predefinito) Attiva immediatamente le configurazioni del controller di gestione, ma posticipa l'attivazione delle configurazioni del server e dell'interfaccia UEFI al successivo riavvio

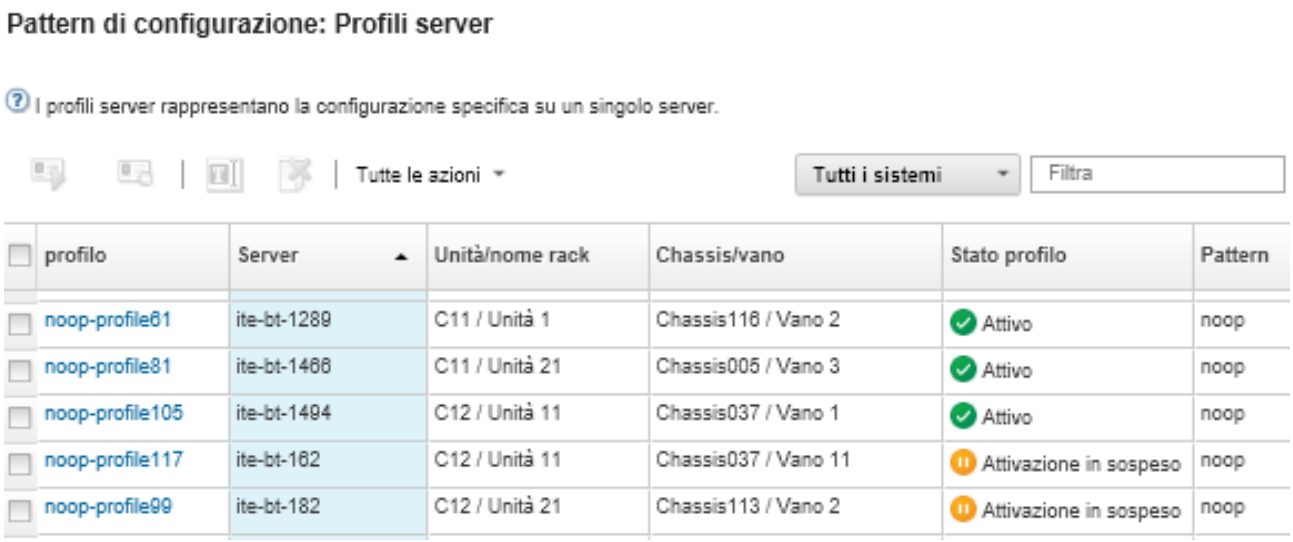
del server. Per l'attivazione completa del profilo è necessario accendere o riavviare manualmente il server.

Nota: Quando si distribuiscono i pattern server che includono solo le impostazioni IMM (incluse le informazioni di sistema, l'interfaccia di gestione e i pattern categoria BMC estesi), non è necessario riavviare il server.

Alla prima attivazione del profilo del server, lo stato del profilo viene modificato in "Attivo." Una volta verificata la conformità, lo stato viene modificato in "Conforme" o "Non conforme."

Risultati

Lo stato del profilo del server nella pagina "Pattern di configurazione: Profili server" viene modificato in "Attivo".



Disattivazione di un profilo del server

È possibile annullare l'assegnazione di un profilo a un server o un vano chassis disattivandolo.

Procedura

Per disattivare un profilo del server, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Profili server**. Viene visualizzata la pagina Pattern di configurazione: Profili server.

Passo 2. Selezionare il profilo del server da disattivare.

Suggerimento: lo stato corrente del profilo del server è elencato nella colonna **Stato profilo**.

Passo 3. Fare clic sull'icona **Disattiva profilo server** ( ).

Passo 4. Scegliere una delle seguenti opzioni di disattivazione:

- **Reimposta impostazioni identità IMM**. Reimposta le impostazioni di identità configurate dal profilo, inclusi il nome host del controller di gestione della scheda di base, il nome del dispositivo e gli indirizzi IP statici assegnati dall'interfaccia di gestione. Verranno reimpostate solo le impostazioni configurate mediante il pattern server associato.

  Nota: Per i server con indirizzi IP assegnati staticamente, questa opzione abilita la modalità DHCP. Se nella rete non è presente un server DHCP abilitato, il server deve essere riconfigurato

manualmente con un indirizzo IP statico valido. Sarà quindi necessario gestire nuovamente i server rack e tower Converged, NeXtScale e System x mediante XClarity Administrator.

- **Spegni il server**. Spegne il server. Alla riaccensione, verranno ripristinati i valori predefiniti integrati delle assegnazioni degli indirizzi virtuali.
- **Forza disattivazione**. Disattiva il profilo del server, anche se il server è stato rimosso o non è raggiungibile.
- **Reimposta le impostazioni delle porte interne dello switch**. Reimposta le impostazioni delle porte interne dello switch configurato dal profilo ai valori predefiniti, inclusa la disabilitazione della modalità UFP e la rimozione delle vport dei membri associati dalle definizioni VLAN. Verranno reimpostate solo le impostazioni configurate mediante il pattern server associato.

  Questa opzione è disabilitata per impostazione predefinita.

  Scegliere questa opzione per non modificare lo stato delle porte dello switch, in cui il profilo del server può essere distribuito su un altro server senza conflitti delle impostazioni con la configurazione precedente delle porte dello switch.

Passo 5. Fare clic su **Disattiva**.

Risultati

Lo stato del profilo del server nella pagina Pattern di configurazione: Profili server passa a Inattivo.

Nota: Se XClarity Administrator non riesce a comunicare con il controller di gestione (ad esempio, se il controller di gestione presenta uno stato di errore o è in fase di riavvio), la disattivazione del profilo del server avrà esito negativo e il profilo non verrà disattivato. In questo caso, ripetere la disattivazione e selezionare l'opzione Forza disattivazione per disattivare il profilo. Il server precedentemente assegnato verrà comunque configurato con le assegnazioni di identità e indirizzi fornite dal profilo. Per evitare conflitti negli indirizzi, è necessario spegnere manualmente il server e rimuoverlo dall'infrastruttura.

Eliminazione di un profilo del server

È possibile eliminare solo i profili dei server che sono stati disattivati.

Prima di iniziare

Verificare che i profili dei server da eliminare siano disattivati (vedere Disattivazione di un profilo del server).

Procedura

Per eliminare un profilo del server, completare la seguente procedura

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Profili server**. Viene visualizzata la pagina Pattern di configurazione: Profili server.

Passo 2. Selezionare il profilo del server il cui stato è "Disattivato".

Suggerimento: lo stato corrente del profilo del server è elencato nella colonna **Stato profilo**.

Passo 3. Fare clic sull'icona **Elimina** ( ).

Nota: Quando si elimina l'ultimo profilo creato, qualsiasi indirizzo WWN o MAC virtuale viene rilasciato dal pool di indirizzi. Se si elimina un profilo che non sia l'ultimo creato, gli indirizzi WWN e MAC virtuali *non* vengono rilasciati dal pool di indirizzi.

Utilizzo di chassis segnaposto

È possibile eseguire il preprovisioning dei server installati in uno chassis di Flex System in un secondo momento, definendo uno *chassis segnaposto* da utilizzare come destinazione del pattern server prima di ricevere l'hardware fisico.

Informazioni su questa attività

In caso di distribuzione di un pattern server in uno chassis segnaposto, Lenovo XClarity Administrator crea un profilo del server per tutti i 14 vani dei server nello chassis di Flex System e riserva gli indirizzi IP di gestione e gli indirizzi Ethernet o Fibre Channel virtuali per i server.

Lo chassis segnaposto aggrega tutti i profili del server, in modo che, una volta ricevuto l'hardware, sarà possibile distribuire lo chassis per attivare i profili sui server fisici, anziché distribuire individualmente tutti i 14 profili. Ciascun server deve essere riavviato per consentire l'attivazione completa del profilo del server.

Creazione di uno chassis segnaposto

Prima di installare l'hardware, è possibile creare uno chassis segnaposto per il preprovisioning. Il provisioning dei nodi di elaborazione dello chassis riserva gli indirizzi IP di gestione e gli indirizzi Ethernet o Fibre Channel virtuali.

Procedura

Per creare uno chassis segnaposto, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Chassis segnaposto**.

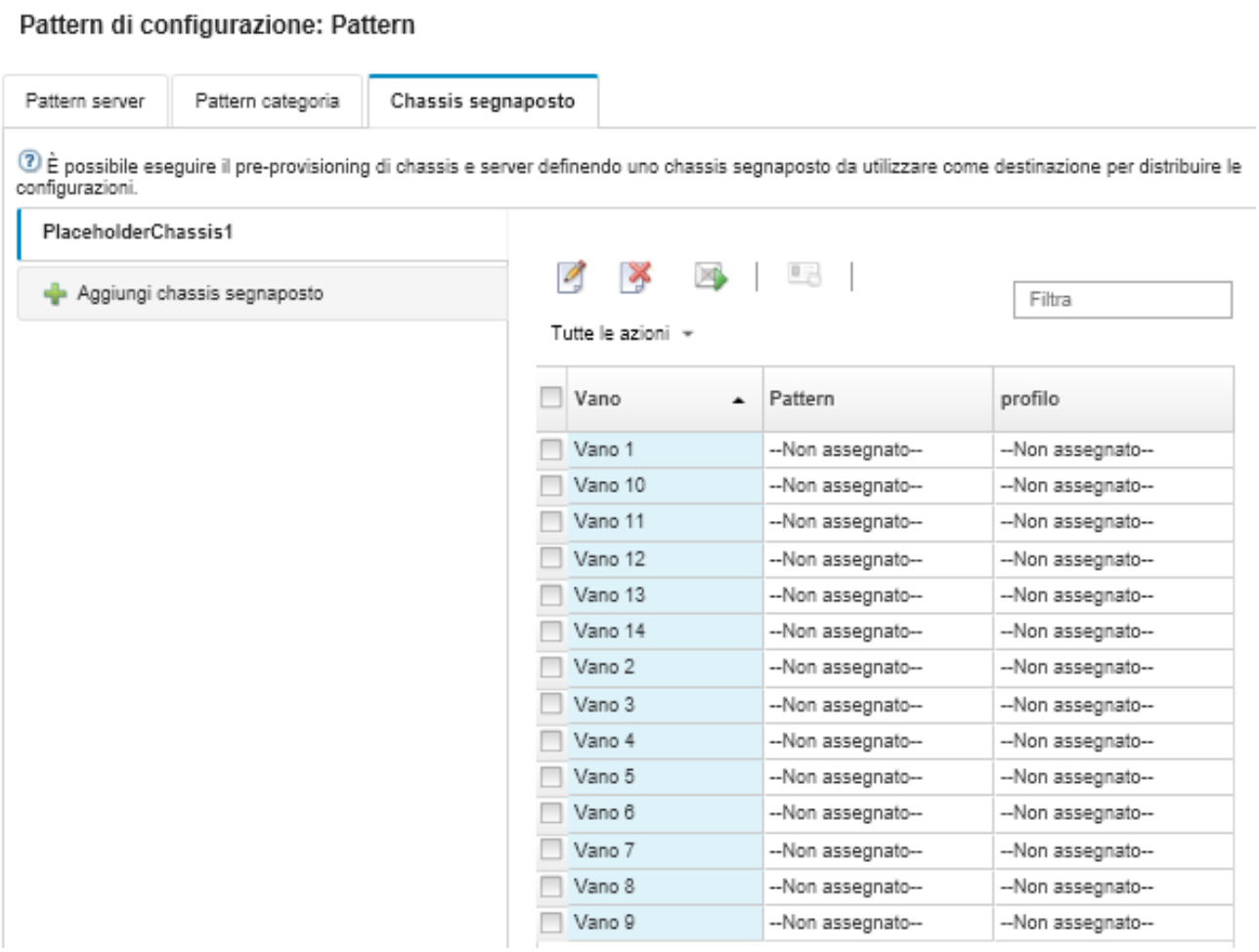
Passo 3. Fare clic sulla linguetta laterale **Aggiungi chassis segnaposto**.

Passo 4. Immettere il nome e la descrizione dello chassis segnaposto.

Passo 5. Fare clic su **Aggiungi**.

Al termine

Una linguetta laterale viene aggiunta al nuovo chassis segnaposto nella pagina Pattern di configurazione: Chassis segnaposto.



Da questa pagina, è possibile eseguire le seguenti azioni su uno chassis segnaposto selezionato:

- Distribuire lo chassis segnaposto facendo clic sull'icona **Distribuisci** ( ).
- Modificare il nome e la descrizione dello chassis segnaposto facendo clic sull'icona **Modifica** ( ).
- Distribuire un pattern server allo chassis segnaposto (vedere Distribuzione di un pattern server in uno chassis segnaposto).
- Disattivare il profilo del server da uno chassis segnaposto (vedere Disattivazione di un profilo del server).
- Eliminare lo chassis segnaposto facendo clic sull'icona **Elimina** ( ).

Distribuzione di un pattern server in uno chassis segnaposto

È possibile distribuire un pattern server in ciascun vano in un uno chassis segnaposto. La distribuzione di un pattern server prima dell'installazione dei server nello chassis di Flex System crea un profilo del server per ciascun vano del server nello chassis e riserva gli indirizzi IP di gestione e gli indirizzi Ethernet o Fibre Channel virtuali.

Procedura

Per distribuire un pattern server in uno chassis segnaposto, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern di configurazione server**. Viene visualizzata la pagina Pattern di configurazione server.

Passo 2. Fare clic sulla scheda **Pattern server**.

Passo 3. Selezionare il pattern server che si desidera distribuire nello chassis segnaposto.

Passo 4. Fare clic sull'icona **Distribuisci** (). Verrà visualizzata la finestra di dialogo Distribuisci pattern server con un elenco degli chassis e degli chassis segnaposto disponibili.

Passo 5. Selezionare **Rinviato** dall'elenco **Attivazione**.

Passo 6. Fare clic su **Mostra vani vuoti**.

Passo 7. Scegliere uno o più vani vuoti dello chassis segnaposto in cui si desidera distribuire il pattern server.

Passo 8. Fare clic su **Distribuisci**. Verrà visualizzata una finestra di dialogo contenente lo stato di distribuzione di ciascun vano selezionato.

Passo 9. Fare nuovamente clic su **Distribuisci** per avviare il processo di distribuzione.

Un profilo del server viene creato e assegnato per ciascun vano selezionato nello chassis segnaposto.

Nota: Il completamento della distribuzione può richiedere alcuni minuti

Passo 10. Fare clic su **Chiudi**.

Al termine

Per monitorare l'avanzamento della distribuzione, fare clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator. È inoltre possibile monitorare la creazione dei profili del server facendo clic su **Provisioning → Profili server**. Al termine della distribuzione, esaminare i profili del server generati e registrare l'indirizzo IP di gestione ed eventuali indirizzi Ethernet o Fibre Channel virtualizzati.

Una volta che lo chassis di Flex System sarà stato fisicamente installato nel rack, quindi rilevato e gestito da XClarity Administrator, sarà possibile distribuire lo chassis segnaposto per effettuare il provisioning di tutti i server nello chassis (vedere Distribuzione di un pattern server in uno chassis segnaposto).

Distribuzione di uno chassis segnaposto

Una volta preconfigurato uno chassis segnaposto mediante la distribuzione di un pattern server e dopo aver rilevato e gestito lo chassis effettivo, sarà possibile distribuire lo chassis segnaposto per configurare gli effettivi nodi di elaborazione.

Procedura

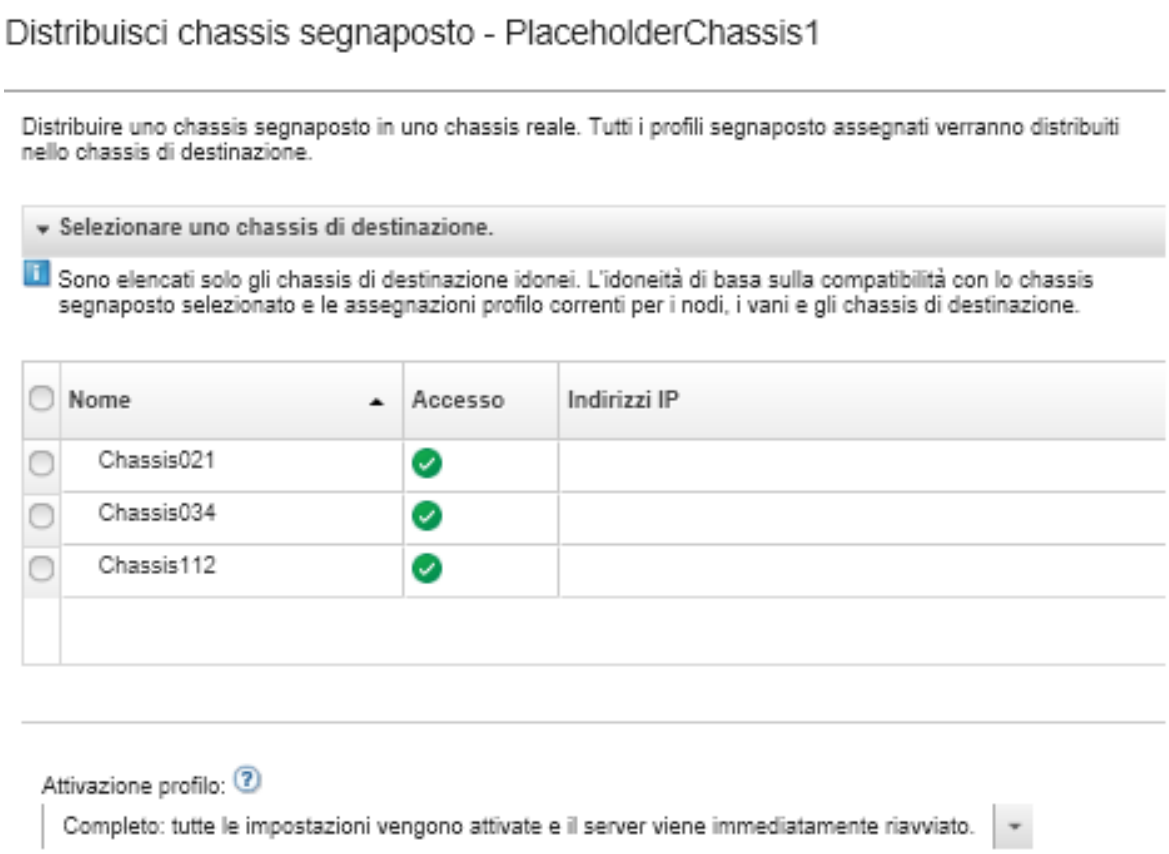
Per distribuire uno chassis segnaposto, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern di configurazione server**. Viene visualizzata la pagina Pattern di configurazione server.

Passo 2. Fare clic sulla scheda **Chassis segnaposto**.

Passo 3. Selezionare la linguetta laterale per lo chassis segnaposto che si desidera distribuire.

Passo 4. Fare clic sull'icona **Distribuisci chassis segnaposto** () per visualizzare la finestra di dialogo Distribuisci chassis segnaposto.



Passo 5. Scegliere quando attivare le configurazioni:

Nota: Subito dopo la distribuzione, le impostazioni di rete nelle relative porte interne dello switch verranno sottoposte al push nello switch, indipendentemente dalla configurazione di attivazione.

- **Completo**. Accende o riavvia immediatamente il server per attivare le configurazioni del server, del controller di gestione della scheda di base e dell'interfaccia UEFI (Unified Extensible Firmware Interface).
- **Parziale**. (predefinito) Attiva immediatamente le configurazioni del controller di gestione, ma posticipa l'attivazione delle configurazioni del server e dell'interfaccia UEFI al successivo riavvio del server. Per l'attivazione completa del profilo è necessario accendere o riavviare manualmente il server.

  Nota: Quando si distribuiscono i pattern server che includono solo le impostazioni IMM (incluse le informazioni di sistema, l'interfaccia di gestione e i pattern categoria BMC estesi), non è necessario riavviare il server.

Passo 6. Fare clic su **Attiva**.

Reimpostazione dei valori predefiniti degli adattatori di storage

È possibile reimpostare le impostazioni predefinite di fabbrica degli adattatori di storage locale di uno o più server.

Informazioni su questa attività

Attenzione: Questa azione cancella tutti i dati sugli adattatori di storage locale.

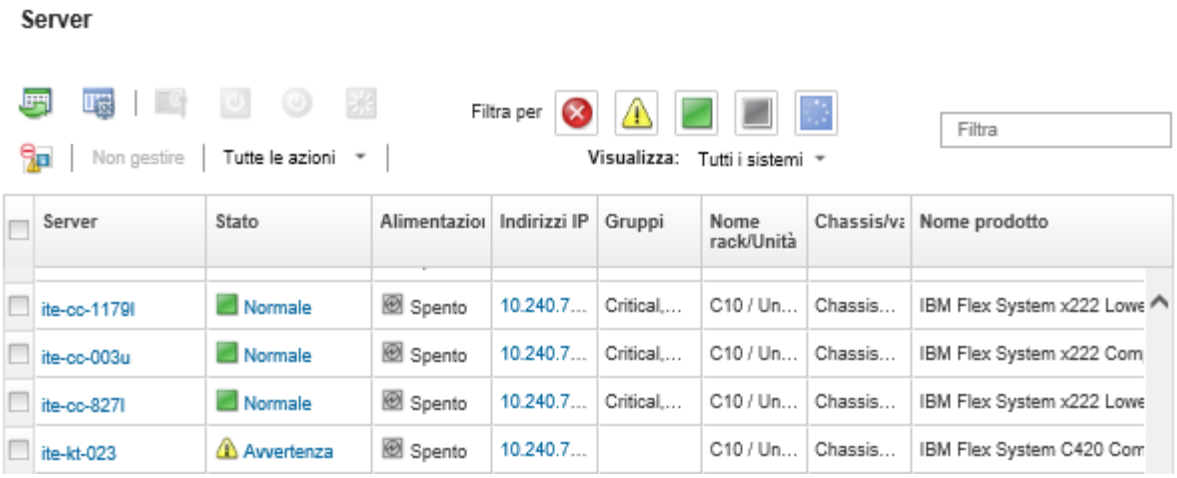
Se il server è spento e il collegamento RAID è supportato, il server viene avviato con la configurazione di sistema per reimpostare gli adattatori delle unità disco fisso e SSD locali.

Procedura

Completare queste operazioni per cancellare la configurazione RAID di uno o più server.

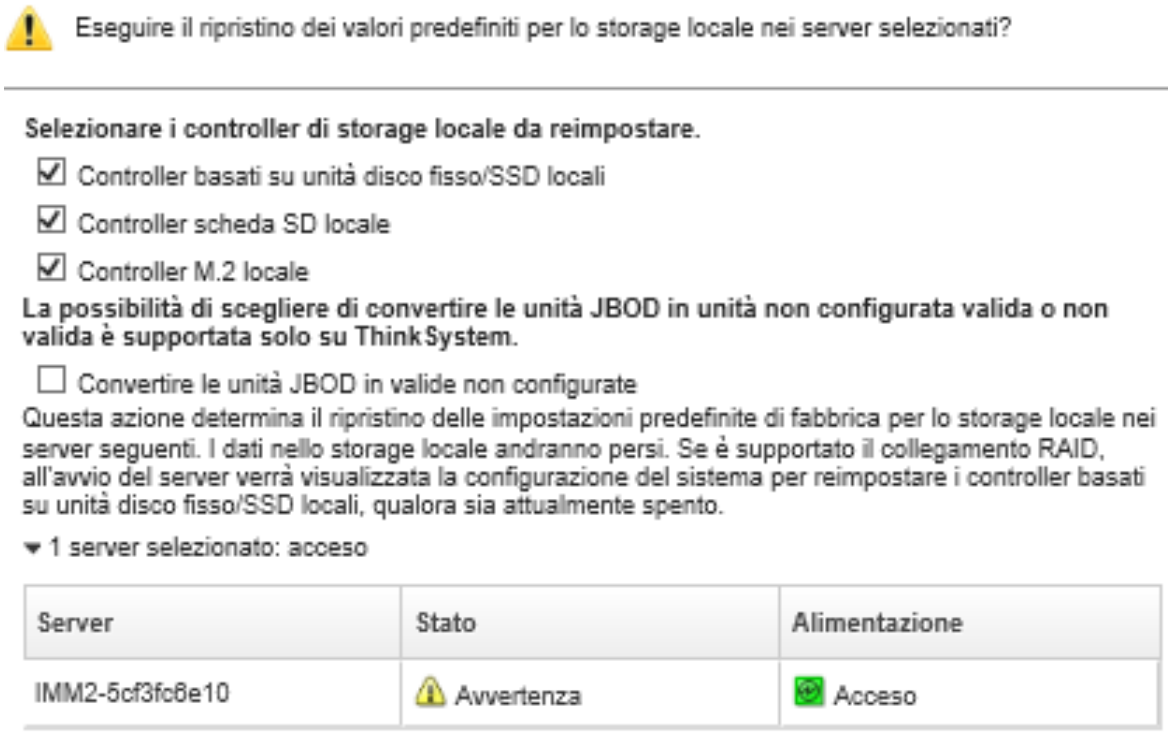
Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Hardware → Server**. Viene visualizzata la pagina Server con una vista tabulare di tutti i server gestiti (server rack e nodi di elaborazione).

È possibile ordinare le colonne della tabella per individuare più facilmente il server che si desidera gestire. Inoltre, è possibile selezionare un tipo di server dall'elenco a discesa **Tutti i sistemi** e immettere del testo (come un nome o un indirizzo IP) nel campo **Filtro** per filtrare ulteriormente i server visualizzati.



Passo 2. Selezionare uno o più server

Passo 3. Selezionare **Tutte le azioni → Servizio → Ripristina valori predefiniti per lo storage locale**. Viene visualizzata una finestra di dialogo in cui vengono richieste ulteriori informazioni.



Passo 4. Selezionare gli adattatori di storage locale da reimpostare.

Passo 5. : (solo server ThinkSystem) Scegliere di convertire le unità JBOD in unità valida non configurata.

Passo 6. Fare clic su **Reimposta storage**.

Configurazione della memoria

È possibile crittografare e decrittare la memoria persistente per i moduli DIMM di memoria Intel® Optane™ DC persistente.

Procedura

Completare la seguente procedura per crittografare e decrittare la memoria persistente.

Passo 1. Dal menu XClarity Administrator, fare clic su **Hardware → Server**. Viene visualizzata la pagina Server con una vista tabulare di tutti i server gestiti (server rack e nodi di elaborazione).

Passo 2. Selezionare uno o più server che si desidera configurare.

Passo 3. Fare clic su **Tutte le azioni → Sicurezza → Operazione Intel Optane PMEM** per visualizzare la finestra di dialogo Operazione Intel Optane PMEM.

Passo 4. Selezionare l'operazione di sicurezza che si desidera eseguire.

- **Abilita sicurezza**. I dati scritti nell'area della memoria persistente vengono crittografati utilizzando la passphrase specificata.

  Importante: Registrare la passphrase di crittografia. La passphrase è necessaria per autorizzare la disabilitazione della sicurezza o la cancellazione della passphrase di crittografia.

- **Disabilita sicurezza**. I dati scritti nell'area della memoria persistente non sono crittografati.

  I dati già memorizzati nell'area della memoria persistente restano crittografati e sono ancora accessibili.

Nota: Questa azione è disponibile solo quando la sicurezza è abilitata ed è impostata la passphrase. È necessario autorizzare questa operazione utilizzando la passphrase corrente. È possibile disabilitare la sicurezza di più moduli DIMM del dispositivo solo se tutti i moduli DIMM condividono la stessa passphrase.

- **Cancellazione sicura**. Cancella la passphrase di crittografia utilizzata per crittografare i dati memorizzati nella regione della memoria persistente per garantire che i dati non siano recuperabili.

  Nota: Questa azione è disponibile solo quando la sicurezza è abilitata ed è impostata la passphrase. È necessario autorizzare questa operazione utilizzando la passphrase corrente.

- **Cancellazione sicura senza passphrase**. Cancella in modo sicuro tutti i dati memorizzati nella memoria persistente dei moduli DIMM specificati nel dispositivo. Dopo la cancellazione sicura, tutti i dati sono irrecuperabili.

  Nota: Questa azione è disponibile solo quando la sicurezza è disabilitata e la passphrase non è richiesta.

Passo 5. Se necessario, specificare e confermare la passphrase.

Passo 6. Fare clic su **OK**.

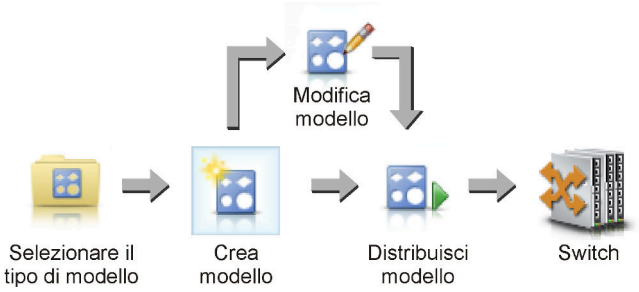
Capitolo 12. Configurazione degli switch mediante i modelli di configurazione

È possibile utilizzare i modelli per eseguire rapidamente il provisioning di più switch rack CNOS da un singolo insieme di impostazioni di configurazione definite.

Informazioni su questa attività

È possibile utilizzare i modelli di configurazione degli switch in XClarity Administrator per configurare le impostazioni globali, i canali delle porte, le reti VLAN, VLAG (Virtual Link Aggregation Group) e le topologie spine-leaf sugli switch gestiti. Attualmente, solo gli switch rack con CNOS sono supportati.

La seguente figura mostra il flusso di lavoro per la configurazione di switch rack gestiti.



1. **Selezionare un tipo di modello.**

   Un *modello di configurazione dello switch* raggruppa le impostazioni correlate degli switch. È possibile creare i seguenti tipi di modelli di configurazione degli switch.
   - **Globale**. Configura le impostazioni globali, come proprietà di sistema, etichette VLAN native e interfacce L2.
   - **Canale porta**. Configura le impostazioni base e avanzate dei canali delle porte, rimuove le porte ed elimina un canale della porta.
   - **Spine-leaf**. Distribuisce una configurazione spine-leaf in una topologia esistente.
   - **VLAN (Virtual LAN)**. Configura le impostazioni e le proprietà VLAN ed elimina una rete VLAN.
   - **VLAG (Virtual Link Aggregation Group)**. Configura le impostazioni VLAG dei peer base e avanzate, crea ed elimina un'istanza del VLAG.
2. **Creare un modello.**

   È possibile creare più modelli di configurazione degli switch per rappresentare configurazioni diverse utilizzate nel data center. I modelli di configurazione degli switch possono essere utilizzati per controllare una configurazione comune di uno switch da un'unica posizione.

   Per ulteriori informazioni sulla creazione di modelli di configurazione degli switch, vedere Creazione di un modello di configurazione dello switch.
3. **Distribuire il modello a uno o più switch.**

   È possibile distribuire un pattern server a uno o più switch rack con CNOS.

   Per ulteriori informazioni sulla distribuzione di una configurazione degli switch, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione.
4. **Modificare un modello.**

   La modifica di un modello di configurazione dello switch non distribuisce automaticamente le impostazioni aggiornate a tutti gli switch a cui è stato distribuito il modello iniziale. È necessario

ridistribuire manualmente i modelli modificati. La pagina della cronologia tiene traccia delle impostazioni per ogni distribuzione.

Impostazione delle preferenze di configurazione del server predefinite

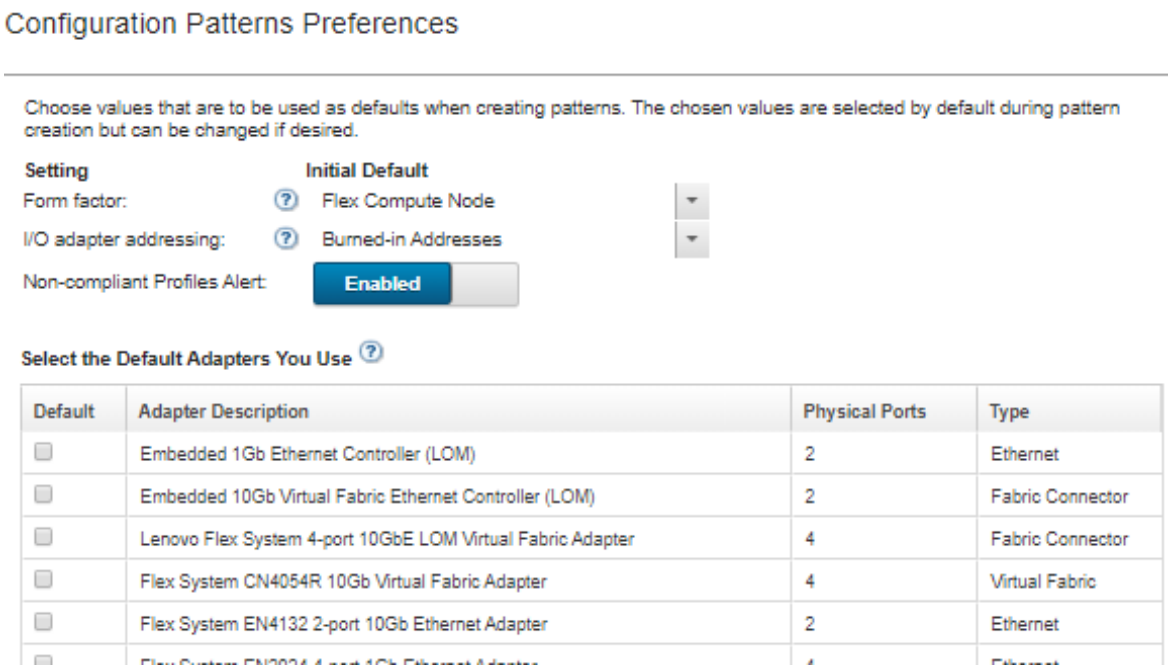
È possibile definire valori selezionati per impostazione predefinita quando si creano pattern di configurazione dei server. I valori possono essere modificati durante la creazione dei pattern server.

Procedura

Per configurare le impostazioni di configurazione del server predefinite, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator fare clic su **Provisioning**, quindi selezionare l'icona Guida (?) accanto a **Pattern di configurazione** per visualizzare la pagina Pattern di configurazione: introduzione.

Passo 2. Fare clic su **Imposta preferenza pattern di configurazione** per visualizzare la finestra di dialogo Preferenza pattern di configurazione.



Passo 3. Selezionare il fattore di forma del server predefinito.

Passo 4. Selezionare la modalità di indirizzamento dell'adattatore I/O predefinita.

- **Integrato**. Utilizzare gli indirizzi WWN (World Wide Name, nome universale) e MAC (Media Access Control) esistenti forniti dal produttore con l'adattatore.
- **Virtuale**. Utilizzare l'indirizzamento dell'adattatore I/O virtuale per semplificare la gestione delle connessioni SAN e LAN. La virtualizzazione degli indirizzi I/O riassegna gli indirizzi hardware integrati con indirizzi WWN Fibre Channel e MAC Ethernet. In questo modo è possibile accelerare la distribuzione preconfigurando l'appartenenza alla zona SAN e agevolare il failover eliminando la necessità di riconfigurare le assegnazioni di suddivisione in zone SAN e mascheramento LUN in fase di sostituzione dell'hardware.

  Se è abilitato l'indirizzamento virtuale, gli indirizzi Ethernet e Fibre Channel sono entrambi allocati per impostazione predefinita, indipendentemente dagli adattatori definiti. È possibile scegliere il pool da cui verranno allocati gli indirizzi Ethernet e Fibre Channel.

È inoltre possibile modificare le impostazioni degli indirizzi virtuali facendo clic sull'icona **Modifica** () accanto alle modalità di indirizzamento.

Limitazione: l'indirizzamento virtuale è supportato solo per i server in chassis di Flex System. Rack e server tower non sono supportati.

Passo 5. Scegliere se abilitare o disabilitare la generazione di un avviso quando le impostazioni di configurazione di un server non corrispondono al profilo di configurazione del server assegnato.

Gli avvisi vengono generati solo per la mancata conformità di un profilo attivo (nello stato ASSIGNED o ERROR_ACTIVATING).

Quando la configurazione del server diventa conforme o se il profilo del server non è assegnato, l'avviso di profilo non conforme viene eliminato.

Passo 6. Selezionare uno o più adattatori I/O predefiniti da utilizzare come adattatori preferiti negli elenchi di selezione.

Passo 7. Fare clic su **Salva**.

Creazione di un modello di configurazione dello switch

Quando si crea un modello di configurazione dello switch vengono definite le impostazioni per un tipo specifico di configurazione.

Prima di iniziare

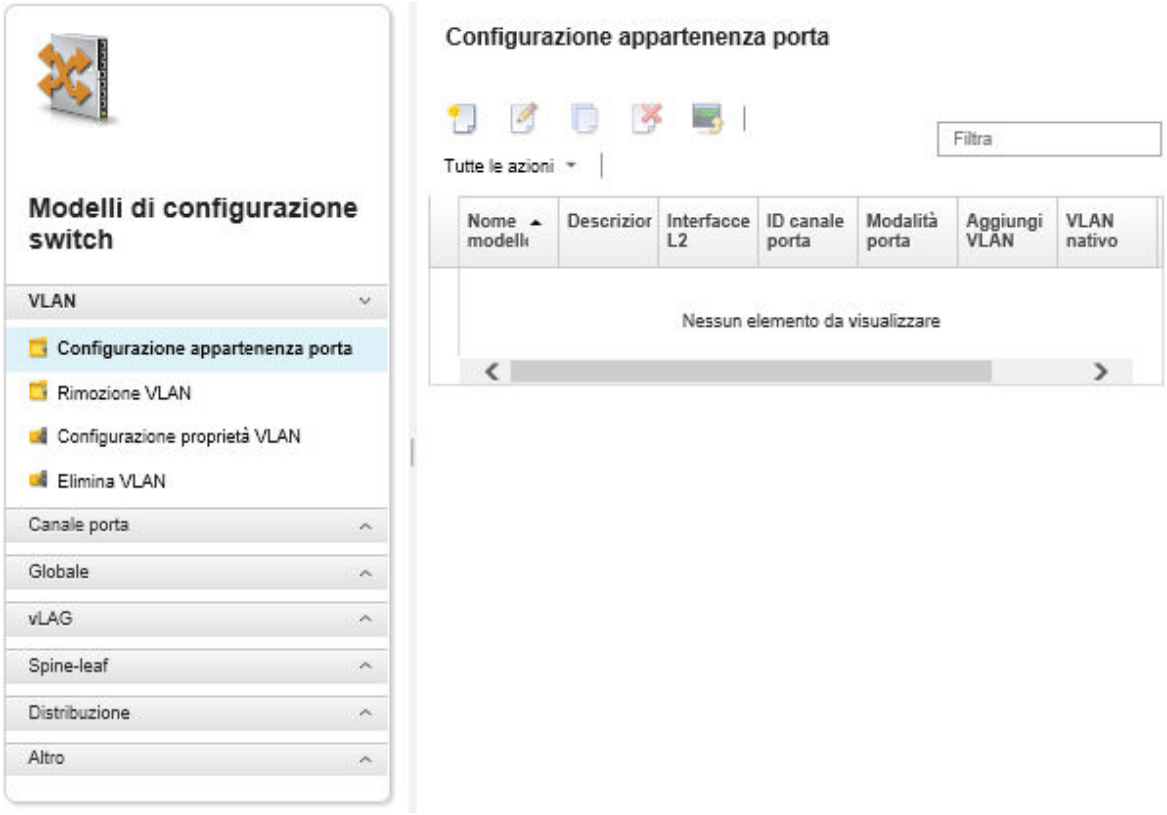
Prima di creare un modello di configurazione degli switch, tenere presente i seguenti suggerimenti:

- Identificare i gruppi di switch con le stesse opzioni hardware e che si desidera configurare allo stesso modo. È possibile utilizzare un modello di configurazione dello switch per applicare le stesse impostazioni di configurazione a più switch, in modo da controllare una configurazione comune da una singola posizione.
- Identificare gli aspetti della configurazione che si desidera personalizzare (ad esempio, globale, porta di canale o impostazioni VLAN).

Procedura

Completare i seguenti passaggi per creare un modello di configurazione dello switch.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".



Passo 2. Selezionare il tipo di modello che si desidera creare nel riquadro di navigazione sinistro.

Passo 3. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo "Crea nuovo modello".

I campi elencati in questa finestra di dialogo variano a seconda del tipo del modello.

Passo 4. Fare clic su **Salva** per salvare il modello oppure su **Salva e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione.

Al termine

Se si è fatto clic su **Salva e distribuisci**, viene visualizzata la pagina "Distribuisci modello switch". Da questa pagina, è possibile distribuire il modello di configurazione dello switch a specifici switch.

Se si è fatto clic su **Salva**, il modello di configurazione dello switch viene salvato nella pagina "Modelli di configurazione switch". Da questa pagina, è possibile eseguire le seguenti azioni sui pattern server selezionati:

- Visualizzare i dettagli sul modello facendo clic sul nome del modello nella colonna "Nome".
- Visualizzare un elenco aggregato di tutti i modelli facendo clic su **Altro → Tutti i modelli**.
- Distribuire il modello (vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione).
- Copiare e quindi modificare un modello facendo clic sull'icona **Copia** ( ).
- Modificare il modello facendo clic sull'icona **Modifica** ( ).

Nota: Le modifiche apportate al modello *non vengono automaticamente* ridistribuite agli switch sui quali era stato distribuito il modello originale.

- Rinominare il pattern, facendo clic sull'icona **Rinomina** ().
- Eliminare il pattern, facendo clic sull'icona **Elimina** ().

Definizione delle impostazioni di appartenenza delle porte VLAN

È possibile aggiungere porte fisiche e canali delle porte a una o più VLAN (per trunk) utilizzando il modello di configurazione di appartenenza delle porte VLAN.

Procedura

Completare le seguenti operazioni per creare un modello di configurazione di appartenenza delle porte.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **VLAN → Configurazione appartenenza porta** nel riquadro di navigazione sinistro, quindi fare clic sull'icona **Crea** ().

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

Importante: È necessario specificare una o più interfacce fisiche L2 o ID del canale della porta.

- Immettere un nome e una descrizione per il modello.
- Specificare una o più interfacce L2 fisiche valide. È possibile specificare un elenco di interfacce separate da una virgola, un intervallo di ID separati da un trattino o una combinazione di entrambi, ad esempio:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Specificare uno o più ID del canale della porta validi (interfacce degli aggregatori porte). È possibile specificare un elenco di numeri separati da una virgola, un intervallo di numeri separati da un trattino o una combinazione di entrambi. I valori e gli intervalli possono essere numeri da 1 a 4.096, ad esempio:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13
- Scegliere se la porta accetta il traffico etichettato o non etichettato. É possibile selezionare uno dei seguenti valori.
  - **accesso**. La porta trasferisce il traffico di una singola rete VLAN.
  - **trunk**. (predefinito) La porta trasferisce il traffico di tutte le reti VLAN accessibili dallo switch.
- Specificare uno o più ID VLAN da aggiungere all'elenco di appartenenza VLAN delle porte. È possibile specificare un elenco di numeri separati da una virgola, un intervallo di numeri separati da un trattino o una combinazione di entrambi. I valori e gli intervalli possono essere numeri da 1 a 4.096, ad esempio:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Nota:

  - Se la modalità della porta è impostata su "accesso", viene utilizzato solo il primo ID VLAN. Ad esempio, nell'intervallo `2-4,5,10-20`, viene utilizzato soltanto `2`.
  - CNOS riserva gli ID VLAN 4.000 - 4.095 per impostazione predefinita. L'utilizzo di ID VLAN riservati (da parte di CNOS o di un altro utente) potrebbe far sì che la distribuzione della configurazione degli switch abbia esito negativo.
- Specificare un ID VLAN nativo utilizzato per applicare un'etichetta al traffico che ne è privo. È possibile utilizzare un numero da 1 a 4.096.

  Nota:
  - Questo campo è valido solo quando la modalità della porta è impostata su "trunk."
  - Se non è specificata, oppure se l'ID è al di fuori dei VLAN di stato finale su una porta, quest'ultima non consentirà il passaggio di traffico non etichettato.
- Selezionare **Crea VLAN** per creare gli ID VLAN che attualmente non sono presenti nello switch di destinazione.

  Se una porta appartiene a una VLAN non creata, la porta continua a essere membro di tale VLAN, ma il traffico etichettato con tale ID VLAN che raggiunge la porta viene bloccato.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Definizione delle proprietà VLAN

È possibile configurare le proprietà VLAN avanzate utilizzando un modello di configurazione delle proprietà della VLAN.

Procedura

Completare le seguenti operazioni per creare un modello di configurazione delle proprietà della VLAN.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **VLAN → Configurazione proprietà VLAN** riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Specificare un ID VLAN cui applicare le modifiche. È possibile utilizzare un numero da 1 a 4.095.

  Nota: CNOS riserva gli ID VLAN 4.000 - 4.095 per impostazione predefinita. L'utilizzo di ID VLAN riservati (da parte di CNOS o di un altro utente) potrebbe far sì che la distribuzione della configurazione degli switch abbia esito negativo.
- Specificare un nome personalizzato per la VLAN.
- Scegliere se le rete VLAN è attiva (abilitata) o sospesa (disabilitata).
- Scegliere se il flooding IP multicast (IPMC) sulla rete VLAN di destinazione è controllato (abilitato) sulle interfacce IPv4 o IPv6. É possibile selezionare uno dei seguenti valori.
  - **Disabilita**. IPv4 e IPv6 sono disabilitati.
  - **Abilita**. IPv4 e IPv6 sono abilitati.
  - **Disabilitazione IPv4**.
  - **Abilitazione IPv4**

- **Disabilitazione IPv6**
- **Abilitazione IPv6**

  Questa azione è additiva, il che significa che "Abilitazione IPv4" distribuita su "Disabilita" dà come risultato "Abilitazione IPv4", ma distribuita su "Abilitazione IPv6" dà invece come risultato "Abilita". Per le opzioni di disabilitazione è vero il contrario.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Rimozione delle impostazioni VLAN

È possibile rimuovere le interfacce dalle VLAN utilizzando il modello di rimozione delle VLAN.

Procedura

Completare le seguenti operazioni per creare un modello di rimozione delle VLAN.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **VLAN → Rimozione VLAN** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

Importante: È necessario specificare una o più interfacce fisiche L2 o ID del canale della porta.

- Immettere un nome e una descrizione per il modello.
- Specificare una o più interfacce L2 fisiche valide. È possibile specificare un elenco di interfacce separate da una virgola, un intervallo di ID separati da un trattino o una combinazione di entrambi, ad esempio:
  - Ethernet1/10
  - Ethernet1/1,3,5,7
  - Ethernet1/1-10,21-30
  - Ethernet2/1-5,7,9,11-13
- Specificare uno o più ID del canale della porta validi (interfacce degli aggregatori porte). È possibile specificare un elenco di numeri separati da una virgola, un intervallo di numeri separati da un trattino o una combinazione di entrambi. I valori e gli intervalli possono essere numeri da 1 a 4.096, ad esempio:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13
- Specificare uno o più ID VLAN da rimuovere dall'elenco di appartenenza VLAN delle porte. È possibile specificare un elenco di numeri separati da una virgola, un intervallo di numeri separati da un trattino o una combinazione di entrambi. I valori e gli intervalli possono essere numeri da 1 a 4.096, ad esempio:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13

Nota: Se la modalità porta è impostata su "accesso", la rimozione della VLAN determina lo spostamento della porta su VLAN 1.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Eliminazione VLAN

È possibile rimuovere le configurazioni VLAN dallo switch utilizzando il modello di eliminazione delle VLAN.

Procedura

Completare le seguenti operazioni per creare un modello di eliminazione delle VLAN.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **VLAN → Elimina VLAN** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Specificare uno o più ID VLAN da rimuovere dall'elenco di appartenenza VLAN delle porte. È possibile specificare un elenco di numeri separati da una virgola, un intervallo di numeri separati da un trattino o una combinazione di entrambi. I valori e gli intervalli possono essere numeri da 1 a 4.096, ad esempio:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Nota: Non è possibile eliminare gli ID VLAN riservati.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Definizione delle impostazioni base dei canali delle porte

È possibile creare aggregatori di porte e aggiungere le porte agli aggregatori mediante un modello di configurazione di base dei canali delle porte.

Se il canale della porta è dotato di porte, e alcune di esse fanno parte del modello, le relative proprietà (priorità della porta, modalità e timeout) vengono aggiornato assieme alle impostazioni del modello quando questo viene distribuito.

Procedura

Completare le seguenti operazioni per creare un modello di configurazione di base dei canali delle porte.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **Canale porta → Configurazione base** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Specificare una o più interfacce L2 fisiche valide. È possibile specificare un elenco di interfacce separate da una virgola, un intervallo di ID separati da un trattino o una combinazione di entrambi, ad esempio:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Specificare l'ID del canale della porta (interfaccia dell'aggregatore porte) da creare o aggiornare. È possibile utilizzare un numero da 1 a 4.095.
- Specificare la modalità della porta LACP (Link Aggregation Control Protocol). É possibile selezionare uno dei seguenti valori.
  - **Attivo**. (predefinito) Abilita LACP incondizionatamente
  - **Passivo**. Abilita LACP solo quando viene rilevato un dispositivo LCAP.
  - **Static**. Disabilita LCAP.

  Nota: Le porte con stato Attivo e Passivo possono essere utilizzate assieme nello stesso aggregatore, contrariamente alle porte con stato Statico.
- Specificare la priorità della porta LACP. È possibile utilizzare un numero da 1 a 65.535.

  Nota: La priorità della porta LACP viene utilizzata con il numero di porta per formare l'ID della porta LACP.
- Specificare la modalità di timeout LACP prima che LCAP entri in modalità singola. É possibile selezionare uno dei seguenti valori.
  - **Lungo**. (predefinito) 90 secondi
  - **Breve**. 3 secondi

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Definizione delle impostazioni avanzate dei canali delle porte

È possibile configurare le proprietà avanzate dei canali delle porte utilizzando un modello di configurazione avanzata dei canali delle porte.

Procedura

Completare le seguenti operazioni per creare un modello di configurazione avanzata dei canali delle porte.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **Canale porta → Configurazione avanzata** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.

- Specificare un ID del canale della porta (interfaccia dell'aggregatore porte) da aggiornare. È possibile utilizzare un numero da 1 a 4.095.
- Scegliere se le singole porte rimangono attive quando LACP non riesce. É possibile selezionare uno dei seguenti valori.
  - **Attivo**. (predefinito) Abilita LACP incondizionatamente.
  - **Sospendi**. Disabilita LACP.
- Specificare il numero minimo di collegamenti che devono essere attivi affinché il canale della porta sia considerato attivo. È possibile utilizzare un numero da 1 a 32.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Eliminazione dei canali delle porte

È possibile rimuovere i canali delle porte dallo switch utilizzando il modello di eliminazione dei canali delle porte.

Procedura

Completare le seguenti operazioni per creare un modello di eliminazione dei canali delle porte.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **Canale porta → Elimina canale porta** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Specificare uno o più ID del canale della porta (interfacce degli aggregatori porte) da eliminare. È possibile specificare un elenco di numeri separati da una virgola, un intervallo di numeri separati da una virgola o una combinazione di entrambi. I valori e gli intervalli possono essere numeri da 1 a 4.096, ad esempio:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Definizione delle impostazioni generali degli switch

È possibile configurare le proprietà generali degli switch utilizzando il modello di configurazione generica globale.

Procedura

Completare le seguenti operazioni per creare un modello di configurazione generica globale degli switch.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **Globale → Configurazione generica** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Specificare la priorità di sistema LACP utilizzata per generare l'ID di sistema LACP. È possibile utilizzare un numero da 1 a 65.535.
- Scegliere dove abilitare l'etichettatura VLAN nativa. É possibile selezionare uno dei seguenti valori.
  - **Ingresso e uscita**
  - **Solo uscita**

  Nota: Questa proprietà è supportata da CNOS 10.10.1 e versioni successive.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Definizione delle impostazioni globali dell'interfaccia L2

È possibile configurare le proprietà di etichettatura VLAN sulle interfacce L2 mediante la configurazione dell'interfaccia L2.

Procedura

Completare le seguenti operazioni per creare un modello di configurazione dell'interfaccia L2.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **Globale → Configurazione interfaccia L2** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Specificare una o più interfacce L2 fisiche valide. È possibile specificare un elenco di interfacce separate da una virgola, un intervallo di ID separati da un trattino o una combinazione di entrambi, ad esempio:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Scegliere dove abilitare l'etichettatura VLAN nativa. É possibile selezionare uno dei seguenti valori.
  - **Ingresso e uscita**
  - **Solo uscita**

  Nota: Questa proprietà è supportata da CNOS 10.10.1 e versioni successive.
- Scegliere se abilitare o disabilitare il supporto per il tunneling (QinQ).

  Nota: Questa proprietà è supportata da CNOS 10.10.1 e versioni successive.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Definizione delle impostazioni VLAG dei peer

È possibile configurare un peer VLAG utilizzando il modello di configurazione dei peer VLAG.

Procedura

Completare le seguenti operazioni per creare un modello di configurazione dei peer VLAG.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **VLAG → Configurazione peer** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Scegliere se abilitare o disabilitare il VLAG.
- Per i peer 1 e 2, completare i seguenti campi. I campi per entrambi i peer devono essere popolati.
  - Specificare l'indirizzo IIPv4 o IPv6 del peer VLAG da utilizzare per il controllo dello stato.
  - Specificare l'ID del canale della porta utilizzato tra i due peer. È possibile utilizzare un numero da 1 a 4.095.
  - Specificare il VRF utilizzato per il controllo dello stato (ad esempio, gestione, impostazione predefinita o customVRF).

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Definizione delle impostazioni delle istanze del VLAG

È possibile creare o aggiornare un'istanza del VLAG utilizzando il modello di configurazione delle istanze del VLAG. Un'istanza del VLAG è un dispositivo collegato a entrambi gli switch (in genere tramite un'aggregazione di porte) che rileva il VLAG come singolo dispositivo.

Procedura

Completare le seguenti operazioni per creare un modello di configurazione delle istanze del VLAG.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **VLAG → Configurazione istanza** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Specificare l'ID VLAG. È possibile utilizzare un numero da 1 a 64.

- Specificare l'ID del canale della porta collegato al peer 1 e 2. È possibile utilizzare un numero da 1 a 4.095.
- Scegliere se abilitare o disabilitare l'istanza del VLAG.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Definizione delle impostazioni VLAG avanzate

È possibile configurare le proprietà VLAG avanzate utilizzando un modello di configurazione avanzata VLAG.

Procedura

Completare le seguenti operazioni per creare un modello di configurazione avanzata VLAG.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **VLAG → Configurazione avanzata** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Specificare la priorità utilizzata per controllare il peer primario. È possibile utilizzare un numero da 1 a 65.535.

  Se non viene specificata alcuna priorità, viene utilizzata la priorità predefinita. Per CNOS, il valore predefinito è 0.
- Specificare il periodo di tolleranza, in secondi, affinché il VLAG torni online dopo un riavvio simultaneo. È possibile utilizzare un numero da 240 a 3.600.

  Se non viene specificato alcun valore, viene utilizzato il valore predefinito dello switch. Per CNOS, il valore predefinito è 300.
- Specificare l'ID livello utilizzato per distinguere le configurazioni VLAG nella stessa rete. È possibile utilizzare un numero da 1 a 512.
- Specificare l'intervallo di ritardo di avvio VLAG, in secondi, utilizzato per ritardare la riattivazione delle porte dopo un ricaricamento del peer. È possibile utilizzare un numero da 0 a 3.600.

  Se non viene specificato alcun valore, viene utilizzato il valore predefinito dello switch. Per CNOS, il valore predefinito è 120.
- Specificare il numero di tentativi keep-alive del VLAG (messaggi "hello" senza risposta) prima che il VLAG sia considerato in stato di errore. È possibile utilizzare un numero da 1 a 24.

  Se non viene specificato alcun valore, viene utilizzato il valore predefinito dello switch. Per CNOS, il valore predefinito è 3.
- Specificare l'intervallo, in secondi, tra i tentativi keep-alive del VLAG. È possibile utilizzare un numero da 2 a 300.

  Se non viene specificato alcun valore, viene utilizzato il valore predefinito dello switch. Per CNOS, il valore predefinito è 5.
- Specificare l'intervallo, in secondi, tra i tentativi ripetuti di keep-alive del VLAG. È possibile utilizzare un numero da 1 a 300.

Se non viene specificato alcun valore, viene utilizzato il valore predefinito dello switch. Per CNOS, il valore predefinito è 30.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Eliminazione di un'istanza del VLAG

È possibile eliminare un'istanza del VLAG creando un modello di eliminazione delle istanze del VLAG.

Procedura

Completare le seguenti operazioni per creare un modello di eliminazione delle istanze del VLAG.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **VLAG → Eliminazione istanza** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Specificare l'ID univoco dell'istanza del VLAG. È possibile utilizzare un numero da 1 a 64.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Definizione di una topologia spine-leaf

È possibile verificare la topologia fisica e distribuire una configurazione SpineLeaf (Fabric L3) sugli switch gestiti mediante il modello di creazione guidata della topologia spine-leaf.

Procedura

Completare le seguenti operazioni per creare un modello di creazione guidata della topologia spine-leaf.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Fare clic su **Spine-Leaf → Creazione guidata topologia** nel riquadro di navigazione sinistro, quindi selezionare l'icona **Crea** ( ).

Passo 3. Nella finestra di dialogo Crea nuovo modello, specificare le seguenti informazioni.

- Immettere un nome e una descrizione per il modello.
- Specificare il numero di sistema autonomo (AS) per il protocollo BGP (Border Gateway Protocol) in esecuzione sullo switch. È possibile utilizzare un numero da 1 a 4.294.967.295.

  Nota: Questa caratteristica è supportata da CNOS 10.9.3 e versioni successive.
- Scegliere se consentire i singoli collegamenti tra gli switch.

  In genere, la distribuzione non riesce se non vi sono almeno due collegamenti tra qualsiasi switch spine e leaf.

Passo 4. Fare clic su **Crea** per salvare il modello oppure su **Crea e distribuisci** per salvare e distribuire immediatamente il modello su uno o più switch rack gestiti.

Per informazioni sulla distribuzione di un modello, vedere Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

Distribuzione di modelli di configurazione degli switch a uno switch di destinazione

È possibile definire le impostazioni delle porte VLAN creando un modello di configurazione delle porte VLAN.

Informazioni su questa attività

Sono disponibili tre tipi di distribuzioni:

- **Normale**. Distribuisce le impostazioni di configurazione dello switch a uno o più switch rack in un'architettura a più livelli base.
- **VLAG**. Distribuisce le impostazioni di configurazione dello switch a due switch che supportano l'architettura VLAG (Virtual Link Aggregation Group). Il modello e la versione software degli switch devono essere identici.
- **Spine-Leaf**. Modelli di distribuzione a uno o più switch spine e leaf.

Procedura

Per distribuire un modello di configurazione degli switch a uno o più switch gestiti, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Selezionare uno o più modelli di configurazione degli switch che si desidera distribuire.

Passo 3. Fare clic sull'icona **Distribuisci** ( ) per visualizzare la finestra di dialogo "Distribuisci modello".

Passo 4. Selezionare uno o più switch a cui si desidera distribuire i modelli.

Vengono elencati solo gli switch compatibili con i modelli selezionati.

Passo 5. Fare clic su **Distribuisci**. Viene visualizzata una finestra di dialogo contenente lo stato di distribuzione di ogni switch selezionato.

Passo 6. Fare nuovamente clic su **Distribuisci** per avviare il processo di distribuzione.

Nota: Il completamento della distribuzione potrebbe richiedere alcuni minuti.

Al termine

È possibile visualizzare la cronologia di distribuzione (vedere Visualizzazione della cronologia di distribuzione delle configurazioni degli switch).

Visualizzazione della cronologia di distribuzione delle configurazioni degli switch

È possibile visualizzare le informazioni sui modelli di configurazione degli switch distribuiti agli switch gestiti, come nome del modello, tipo di modello, timestamp e gli switch a cui sono stati distribuiti. Ciascuna distribuzione contiene un'istantanea del modello al momento della distribuzione.

Procedura

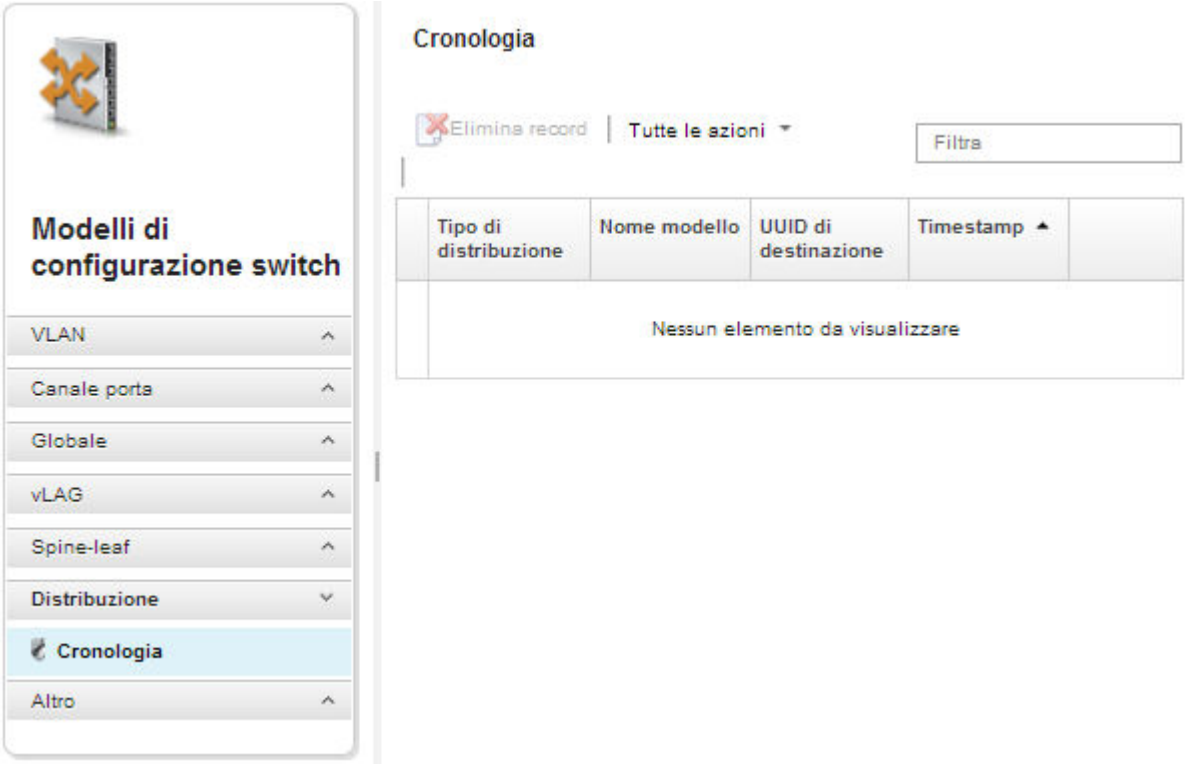
Completare le seguenti operazioni per visualizzare la cronologia di distribuzione delle configurazioni degli switch.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Modelli di configurazione switch**. Viene visualizzata la pagina "Modelli di configurazione switch".

Passo 2. Espandere **Distribuzione**, quindi fare clic su **Cronologia** nel riquadro di navigazione sinistro per visualizzare una tabella dei modelli distribuiti.

La colonna **Stato** indica se la distribuzione della configurazione ha avuto esito positivo. Può contenere uno dei seguenti valori di stato:

- **Riuscito**. La distribuzione della configurazione a tutti gli switch di destinazione è stata completata correttamente.
- **Avvertenza**. La distribuzione della configurazione a uno o più switch di destinazione è stata completata con avvisi.
- **Non riuscito**. La distribuzione della configurazione a uno o più switch di destinazione non è riuscita.



Al termine

- Per visualizzare le informazioni su ciascun modello distribuito, inclusi gli elementi distribuiti e il relativo esito, fare clic sul nome del modello nella tabella.
- Cancellare la cronologia delle distribuzioni selezionando una distribuzione e facendo clic sull'icona **Elimina** ( ).

Capitolo 13. Aggiornamento del firmware sui dispositivi gestiti

Dall'interfaccia Web di Lenovo XClarity Administrator è possibile scaricare, installare e gestire aggiornamenti firmware per i dispositivi gestiti, inclusi chassis, server, sistemi di storage e switch. È possibile assegnare criteri di conformità del firmware ai dispositivi gestiti per garantirne la conformità. È anche possibile creare e modificare criteri di conformità del firmware quando i livelli di firmware convalidati non corrispondono ai criteri predefiniti consigliati.

Ulteriori informazioni:
- XClarity Administrator: aumento dell'efficenza durante l'aggiornamento del firmware
- Procedure ottimali per l'aggiornamento di driver e firmware di Lenovo ThinkSystem
- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: aggiornamenti firmware
- XClarity Administrator: provisioning degli aggiornamenti di sicurezza del firmware

Prima di iniziare

L'aggiornamento del firmware e dei driver di dispositivo sono processi separati in XClarity Administrator; questi processi non sono in alcun modo connessi. XClarity Administrator non gestisce la conformità tra il firmware e i driver dei dispositivi sui dispositivi gestiti, anche se si consiglia di aggiornare i driver di dispositivo contemporaneamente al firmware.

Informazioni su questa attività

Nota: Non è necessario un sistema operativo per aggiornare il firmware. Per i server bare metal, verificare che il server sia spento prima di aggiornare il firmware.

È possibile gestire e applicare gli aggiornamenti firmware ai seguenti dispositivi gestiti.
- **Chassis**. Aggiornamenti CMM
- **Server ThinkAgile, ThinkSystem, System x, Converged, Flex System e NeXtScale**. Aggiornamenti di Baseboard Management Controller, UEFI, DSA, mezzanino e adattatore
- **Switch RackSwitch e Flex System**
- **Dispositivi di storage Lenovo Storage e ThinkSystem DM**
- **Dispositivi della libreria a nastro IBM TS4300**

Il firmware per i seguenti dispositivi non può essere aggiornato tramite XClarity Administrator.

- **Server ThinkServer**. Consultare la documentazione fornita con il server per trovare informazioni su come aggiornare il firmware.
- **Nodi di elaborazione Flex Power Systems**. Sono disponibili diversi metodi per aggiornare il firmware per i nodi di elaborazione Flex Power Systems. Per ulteriori informazioni, vedere Documentazione online dei nodi di elaborazione IBM Flex System p260/p460. Il processo per gli altri nodi di elaborazione Flex Power Systems è simile.
- **Switch Flex in modalità impilata o protetta**. *Non è possibile* aggiornare il firmware sugli switch impilati. L'aggiornamento del firmware è disabilitato per tutti gli switch impilati.
- **Switch Flex**. Se si utilizzano gli switch elencati di seguito, consultare la documentazione fornita con lo switch per trovare informazioni su come aggiornare il firmware.
  - Cisco Nexus B22 Fabric Extender

Procedura

La seguente figura mostra il flusso di lavoro per l'aggiornamento del firmware sui dispositivi gestiti.

Passo 1. **Gestione del repository degli aggiornamenti firmware**

Il *repository degli aggiornamenti firmware* contiene un catalogo di aggiornamenti disponibili e i pacchetti di aggiornamento applicabili ai dispositivi gestiti.

Il *catalogo* contiene informazioni relative agli aggiornamenti firmware attualmente disponibili per tutti i dispositivi supportati da XClarity Administrator. Il catalogo organizza gli aggiornamenti firmware per tipo di dispositivo. Quando si aggiorna il catalogo, XClarity Administrator recupera le informazioni sugli ultimi aggiornamenti firmware disponibili dal sito Web di Lenovo (inclusi i file metadata.xml o .json e readme.txt) e le archivia nel repository degli aggiornamenti firmware. Il file di payload (.exe) non è stato scaricato. Per ulteriori informazioni sull'aggiornamento del catalogo, vedere Aggiornamento del catalogo prodotti.

Se sono disponibili nuovi aggiornamenti firmware, è necessario scaricare i pacchetti di aggiornamento prima di aggiornare il firmware sui dispositivi gestiti. L'aggiornamento del catalogo non include il download automatico dei pacchetti di aggiornamento. La tabella **Catalogo prodotti** nella pagina Repository aggiornamenti firmware identifica i pacchetti di aggiornamento scaricati e quelli disponibili per il download.

È possibile scaricare gli aggiornamenti firmware in diversi modi:

- **Pacchetti del repository degli aggiornamenti firmware**

  I pacchetti del repository degli aggiornamenti firmware sono raccolte del firmware più recente che è disponibile contemporaneamente al rilascio di XClarity Administrator per molti dispositivi supportati, nonché criteri di conformità del firmware predefiniti. Questi pacchetti del repository vengono importati e successivamente applicati attraverso la pagina Aggiorna server di gestione. Quando si applica un pacchetto del repository degli aggiornamenti firmware, ogni pacchetto di aggiornamento viene aggiunto al repository degli aggiornamenti firmware e vengono creati automaticamente criteri di gestione del firmware per tutti i dispositivi gestibili. Questo criterio predefinito può essere copiato ma non modificato.

  Sono disponibili i seguenti pacchetti del repository.

  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i CMM e gli switch Flex System.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per tutti gli switch RackSwitch e i dispositivi Lenovo Storage.
  - **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per i server Converged serie HX, Flex System, NeXtScale e System x.
  - **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i server ThinkAgile e ThinkSystem.
  - **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i server ThinkAgile e ThinkSystem V2.
  - **lnvgy_sw_lxca_thinksystemv3repo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i server ThinkAgile e ThinkSystem V3.

È possibile determinare se i pacchetti del repository degli aggiornamenti firmware vengono memorizzati nel repository verificando il valore della colonna **Stato download** nella pagina Aggiorna server di gestione. Questa colonna contiene i seguenti valori:

- **Scaricato**. Il pacchetto del repository degli aggiornamenti firmware è memorizzato nel repository.
- **Non scaricato**. Il pacchetto del repository degli aggiornamenti firmware è disponibile ma non è memorizzato nel repository.

- **UpdateXpress System Packs (UXSPs)**

  Nota: Per i server con XCC2, questi pacchetti vengono definiti bundle di firmware. Il *bundle* viene utilizzato nei nomi dei pacchetti e nei nomi dei criteri predefiniti.

  I pacchetti UXSP contengono i più recenti aggiornamenti disponibili dei driver di dispositivo e dei firmware, organizzati per sistema operativo. Quando si scaricano i pacchetti UXSP, XClarity Administrator scarica il pacchetto UXSP in base alla versione elencata nel catalogo e memorizza i pacchetti di aggiornamento nel repository degli aggiornamenti firmware. Quando si scarica un pacchetto UXSP, ogni aggiornamento firmware in UXSP viene aggiunto al repository degli aggiornamenti firmware ed elencato nella scheda **Aggiornamenti individuali** e vengono creati automaticamente criteri di conformità del firmware per tutti i dispositivi gestibili utilizzando i seguenti nomi. Questo criterio predefinito può essere copiato ma non modificato.
  - *{uxsp-version}-{date}-{server-short-name}***-UXSP** (ad esempio, `v1.50-2017-11-22- SD530-UXSP`)
  - *{uxsp-version}-{buildnumber}-{server-short-name}***-bundle** (ad esempio, `22a.0-kaj92va-SR650V3-bundle`)

  Nota: Quando si scaricano o si importano i pacchetti UXSPs dalla pagina Aggiornamenti firmware: Repository, solo gli aggiornamenti firmware vengono scaricati e memorizzati nel repository. Gli aggiornamenti dei driver di dispositivo vengono ignorati. Per informazioni sul download o l'importazione dei driver di dispositivo di Windows mediante i pacchetti UXSPs, vedere Gestione del repository dei driver di dispositivo del sistema operativo.

  È possibile determinare se i pacchetti UXSPs vengono archiviati nel repository degli aggiornamenti firmware nella colonna **Stato del download** nella scheda **Aggiornamenti individuali** della pagina Aggiornamenti firmware: Repository. Questa colonna contiene i seguenti valori:

  - **Scaricato**. L'intero pacchetto di aggiornamento o i singoli aggiornamenti firmware vengono memorizzati nel repository.
  - *x* **di** *y* **Scaricato**. Non tutti gli aggiornamenti firmware nel pacchetto di aggiornamento sono memorizzati nel repository. I numeri tra parentesi indicano il numero di aggiornamenti disponibili e il numero di aggiornamenti memorizzati, oppure l'indisponibilità di aggiornamenti per il tipo di dispositivo specifico.
  - **Non scaricato**. L'intero pacchetto di aggiornamento o i singoli aggiornamenti firmware sono disponibili ma non sono memorizzati nel repository.

- **Aggiornamenti firmware individuali**

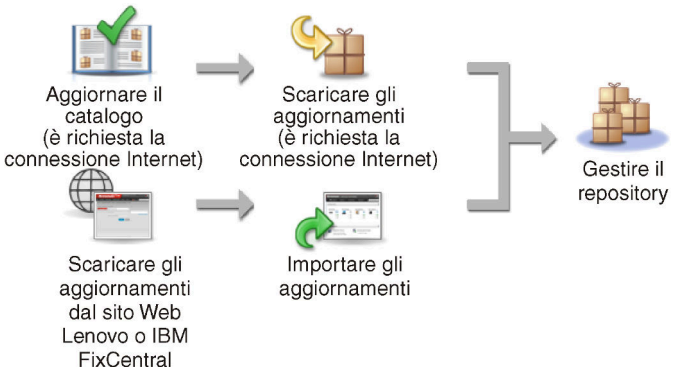
  È possibile scaricare i singoli pacchetti di aggiornamento firmware individuali. Quando si scaricano i pacchetti di aggiornamento firmware, XClarity Administrator scarica l'aggiornamento in base alla versione elencata nel catalogo e memorizza i pacchetti di aggiornamento nel repository degli aggiornamenti firmware. È possibile quindi creare i criteri di conformità del firmware utilizzando tali pacchetti di aggiornamento per ciascuno dei dispositivi gestiti.

Nota: Gli aggiornamenti firmware principali (come il controller di gestione, UEFI e pDSA) sono indipendenti del sistema operativo. I pacchetti di aggiornamento firmware per i sistemi operativi RHEL 6 o SLES 11 sono utilizzati per aggiornare i nodi di elaborazione e i server rack. Per ulteriori informazioni sui pacchetti di aggiornamento firmware da utilizzare per i server gestiti, vedere Download degli aggiornamenti firmware.

È possibile determinare se gli specifici *aggiornamenti firmware* vengono memorizzati nel repository degli aggiornamenti firmware verificando il valore della colonna **Stato del download** nella scheda **Aggiornamenti individuali** della pagina Aggiornamenti firmware: Repository. Questa colonna contiene i seguenti valori.

- **Scaricato**. L'intero pacchetto di aggiornamento o i singoli aggiornamenti firmware vengono memorizzati nel repository.
- *x* **di** *y* **Scaricato**. Non tutti gli aggiornamenti firmware nel pacchetto di aggiornamento sono memorizzati nel repository. I numeri tra parentesi indicano il numero di aggiornamenti disponibili e il numero di aggiornamenti memorizzati, oppure l'indisponibilità di aggiornamenti per il tipo di dispositivo specifico.
- **Non scaricato**. L'intero pacchetto di aggiornamento o i singoli aggiornamenti firmware sono disponibili ma non sono memorizzati nel repository.

XClarity Administrator deve essere collegato a Internet per aggiornare il catalogo e scaricare gli aggiornamenti firmware. Se non è collegato a Internet, è possibile scaricare manualmente i file in una workstation che ha accesso alla rete nell'host XClarity Administrator, tramite un browser Web e quindi importare i file nel repository degli aggiornamenti firmware.



Quando si importano manualmente gli aggiornamenti firmware in XClarity Administrator, è necessario includere i seguenti file: payload (immagine e MIB), metadati, cronologia delle modifiche e readme. Ad esempio:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Attenzione:

- Importare solo questi file obbligatori. Non importare altri file che potrebbero essere disponibili nei siti Web di download del firmware.
- Se non si include il file XML nel pacchetto di aggiornamento, l'aggiornamento non viene importato.
- Se non si includono tutti i file richiesti associati all'aggiornamento, il repository contrassegna l'aggiornamento come non scaricato, ad indicare che è stato parzialmente importato. È quindi possibile importare i file mancanti selezionandoli e importandoli.

- Gli aggiornamenti firmware principali (come il controller di gestione, UEFI e pDSA) sono indipendenti del sistema operativo. I pacchetti di aggiornamento firmware per i sistemi operativi RHEL 6 o SLES 11 sono utilizzati per aggiornare i nodi di elaborazione e i server rack. Per ulteriori informazioni sui pacchetti di aggiornamento firmware da utilizzare per i server gestiti, vedere Download degli aggiornamenti firmware.

Per ulteriori informazioni sugli aggiornamenti firmware, vedere Gestione del repository degli aggiornamenti firmware.

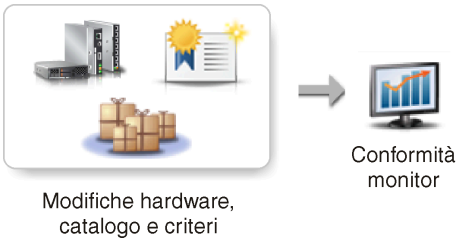
Passo 2. **(Facoltativo) Creazione e assegnazione di criteri di conformità del firmware**

I *criteri di conformità del firmware* permettono di verificare che il livello di firmware di determinati dispositivi gestiti sia al livello corrente o specificato, contrassegnando i dispositivi che richiedono attenzione. Ogni criterio di conformità del firmware identifica i dispositivi monitorati e il livello firmware da installare per mantenere la conformità dei dispositivi. È possibile impostare la conformità a livello di dispositivo o componente firmware. XClarity Administrator utilizza quindi questi criteri per controllare lo stato dei dispositivi gestiti e identificare i dispositivi non conformi.

Quando si creano dei criteri di conformità del firmware, è possibile configurare XClarity Administrator in modo che contrassegni un dispositivo nei seguenti casi:
- Il firmware del dispositivo è di livello inferiore a quello richiesto
- Il firmware del dispositivo non corrisponde esattamente alla versione dell'obiettivo di conformità

XClarity Administrator è dotato di criteri di conformità del firmware predefiniti denominati **Firmware più recente nel repository**. Quando il nuovo firmware viene scaricato o importato nel repository, questo criterio viene aggiornato per includere le versioni di firmware più recenti nel repository.

Una volta assegnati a un dispositivo i criteri di conformità del firmware, XClarity Administrator verifica lo stato di conformità di ogni dispositivo ogni volta che vengono apportate modifiche all'inventario del dispositivo o a un repository degli aggiornamenti firmware. Quando il firmware di un dispositivo non è conforme ai criteri assegnati, XClarity Administrator identifica il dispositivo come non conforme nella pagina Aggiornamenti firmware: Applica/Attiva, in base alla regola specificata nei criteri di conformità del firmware.



Ad esempio, è possibile creare criteri di conformità del firmware che definiscono il livello di riferimento per il firmware installato in tutti i dispositivi ThinkSystem SR850 e quindi assegnare i criteri di conformità del firmware a tutti i dispositivi ThinkSystem SR850 gestiti. Quando il repository degli aggiornamenti firmware viene aggiornato e viene aggiunto un nuovo aggiornamento firmware, tali nodi di elaborazione potrebbero diventare non conformi. Quando ciò si verifica, XClarity Administrator aggiorna la pagina Aggiornamenti firmware: Applica/Attiva per contrassegnare tali dispositivi come non conformi e genera un avviso.

Nota: È possibile scegliere di visualizzare o nascondere gli avvisi per i dispositivi che non soddisfano i requisiti dei criteri di conformità del firmware assegnati (vedere Configurazione delle impostazioni globali di aggiornamento del firmware). Gli avvisi vengono nascosti per impostazione predefinita.

Per ulteriori informazioni sui criteri di conformità del firmware, vedere Creazione e assegnazione di criteri di conformità del firmware.

Passo 3. **Applicazione e attivazione degli aggiornamenti**

XClarity Administrator non applica automaticamente gli aggiornamenti firmware ai dispositivi gestiti. Per aggiornare il firmware, è necessario applicare e attivare manualmente l'aggiornamento sui dispositivi selezionati. È possibile applicare il firmware utilizzando uno dei seguenti metodi.

- **Applicare gli aggiornamenti firmware in bundle utilizzando i criteri di conformità**

  È possibile applicare gli aggiornamenti firmware a *tutti* i componenti dei dispositivi selezionati in base ai criteri di conformità del firmware assegnati utilizzando un'immagine del bundle che contiene i pacchetti di aggiornamento firmware applicabili.

  Il processo di aggiornamento in bundle aggiorna innanzitutto il controller di gestione della scheda di base e UEFI fuori banda. Al termine degli aggiornamenti, il processo crea un'immagine in bundle del firmware restante nei criteri di conformità in base al tipo di macchina. Quindi, il processo monta l'immagine sul dispositivo selezionato e riavvia il dispositivo per avviare l'immagine. L'immagine viene eseguita automaticamente per completare gli aggiornamenti rimanenti.

  Attenzione: I dispositivi selezionati verranno spenti prima di avviare il processo di aggiornamento. Verificare che qualsiasi carico di lavoro in esecuzione venga interrotto oppure, se si lavora in un ambiente virtualizzato, venga spostato su un server differente. Se sono in esecuzione dei processi, il processo di aggiornamento viene messo in coda fino al completamento di tutti gli altri processi. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio → Processi**.

  Nota:

  – L'applicazione degli aggiornamenti firmware in bundle è supportata solo per i server ThinkSystem SR635 e SR655.

  – L'applicazione di aggiornamenti firmware in bundle è supportata solo per l'indirizzo IPv4. Gli indirizzi IPv6 non sono supportati.

  – Verificare che ciascun dispositivo di destinazione sia stato avviato nel sistema operativo almeno una volta per recuperare le informazioni complete dell'inventario.

  – Per utilizzare la funzione di aggiornamento in bundle è richiesto il firmware del controller di gestione della scheda di base v2.94 o versione successiva.

  – Vengono utilizzati solo gli aggiornamenti firmware dei pacchetti del repository o i singoli aggiornamenti firmware. I pacchetti UpdateXpress System Packs (UXSPs) non sono supportati.

  – Solo gli aggiornamenti firmware scaricati vengono applicati. Aggiornare il catalogo prodotti e scaricare gli aggiornamenti firmware appropriati (vedere Aggiornamento del catalogo prodotti e Download degli aggiornamenti firmware).

    Nota: Quando XClarity Administrator viene installato per la prima volta, il catalogo prodotti e il repository sono vuoti.

  – Il controllo di conformità è supportato solo per il controller di gestione della scheda di base e UEFI nei server ThinkSystem SR635 e SR655. XClarity Administrator tenta comunque di applicare gli aggiornamenti firmware a tutti i componenti hardware disponibili.

  – Gli aggiornamenti vengono applicati in base ai criteri di conformità del firmware assegnati. Non è possibile scegliere di aggiornare un sottoinsieme di componenti.

- XClarity Administrator v3.2 o versione successiva è richiesto per applicare gli aggiornamenti firmware per Lenovo XClarity Provisioning Manager (LXPM), i driver Windows LXPM o i driver Linux LXPM ai server ThinkSystem SR635 e SR655.
- Gli aggiornamenti del controller di gestione della scheda di base e UEFI vengono ignorati se la versione attualmente installata è superiore ai criteri di conformità assegnati.
- I criteri di conformità del firmware devono essere creati e assegnati ai dispositivi ai quali si desidera applicare gli aggiornamenti firmware. Per ulteriori informazioni, vedere Creazione e assegnazione di criteri di conformità del firmware.
- I dispositivi selezionati verranno spenti prima di avviare il processo di aggiornamento. Verificare che qualsiasi carico di lavoro in esecuzione venga interrotto oppure, se si lavora in un ambiente virtualizzato, venga spostato su un server differente.

- **Applicare gli aggiornamenti firmware selezionati con o senza criteri di conformità**

  È possibile applicare gli aggiornamenti firmware sui componenti e i dispositivi selezionati in base ai criteri di conformità del firmware assegnati utilizzando i pacchetti di aggiornamento firmware applicabili. È inoltre possibile scegliere di applicare aggiornamenti firmware superiori rispetto a quello attualmente installato nei componenti e i dispositivi selezionati senza utilizzare criteri di conformità.

  È possibile scegliere di applicare gli aggiornamenti per tutti i componenti in uno specifico dispositivo. È anche possibile scegliere di aggiornare solo un sottoinsieme di componenti nei dispositivi selezionati, quali il controller di gestione della scheda di base o UEFI.

  Per attivare gli aggiornamenti firmware occorre riavviare i dispositivi. (il riavvio di un dispositivo comporta l'interruzione di tutte le operazioni in corso). È possibile scegliere di riavviare i dispositivi nell'ambito del processo di aggiornamento (denominata *attivazione immediata*) oppure attendere la disponibilità di una finestra di manutenzione per il riavvio dei dispositivi (*attivazione ritardata*). In questo caso, è necessario riavviare manualmente il dispositivo affinché l'aggiornamento abbia effetto.

  Quando si sceglie di aggiornare il firmware per un dispositivo gestito, vengono eseguite le seguenti operazioni.

  1. XClarity Administrator invia gli aggiornamenti firmware (ad esempio, per il controller di gestione, per UEFI e DSA) al dispositivo.
  2. Quando il dispositivo viene riavviato, gli aggiornamenti firmware vengono attivati sul dispositivo.
  3. Per i server, XClarity Administrator invia gli aggiornamenti per i dispositivi opzionali, ad esempio gli aggiornamenti per la scheda di rete e l'unità disco fisso. XClarity Administrator applica tali aggiornamenti e il server viene riavviato.
  4. Quando si riavvia il dispositivo o si sceglie l'attivazione immediata, gli aggiornamenti per i dispositivi opzionali vengono attivati.

  Nota:

  - Quando si applicano gli aggiornamenti utilizzando i criteri di conformità è necessario creare e assegnare criteri di conformità del firmware a ciascun dispositivo di destinazione. Per ulteriori informazioni, vedere Creazione e assegnazione di criteri di conformità del firmware.
  - Se si sceglie di installare un pacchetto di aggiornamento firmware che contiene aggiornamenti per più componenti, vengono aggiornati tutti i componenti a cui viene applicato il pacchetto di aggiornamento.
  - Gli aggiornamenti ai CMM e agli switch Flex vengono sempre attivati immediatamente, anche se si sceglie l'attivazione ritardata.

Quando si eseguono aggiornamenti su una serie di dispositivi, XClarity Administrator esegue gli aggiornamenti nel seguente ordine.

- CMM chassis
- Switch RackSwitch e Flex System
- Nodi di elaborazione Flex, server tower e rack
- Dispositivi Lenovo Storage

Attenzione: Prima di tentare di applicare gli aggiornamenti firmware sui dispositivi gestiti, assicurarsi di aver completato le seguenti operazioni.

- Leggere le considerazioni sull'aggiornamento del firmware prima di tentare di aggiornare il firmware sui dispositivi gestiti (vedere Considerazioni sugli aggiornamenti firmware).
- Inizialmente, i dispositivi non supportati dagli aggiornamenti non vengono visualizzati. Non è possibile selezionare i dispositivi non supportati dagli aggiornamenti.
- Per impostazione predefinita, tutti i componenti rilevati sono elencati come disponibili per l'applicazione degli aggiornamenti; tuttavia, la presenza di firmware di livello inferiore potrebbe far sì che un componente non venga visualizzato nell'inventario o non presenti informazioni complete sulla versione. Per visualizzare l'elenco di tutti i pacchetti basati su criteri disponibili per l'applicazione di aggiornamenti, fare clic sull'icona **Tutte le azioni → Impostazioni globali** e selezionare **Supporto potenziato per dispositivi di livello inferiore**. Quando questa opzione è selezionata, la voce "Altro software disponibile" è riportata nella colonna Versione installata per i dispositivi non rilevati. Per ulteriori informazioni, vedere Configurazione delle impostazioni globali di aggiornamento del firmware.

  Nota:

  – Le impostazioni globali non possono essere modificate se sono in corso aggiornamenti ai dispositivi gestiti.

  – La generazione delle opzioni aggiuntive richiede alcuni minuti. Dopo alcune informazioni, potrebbe essere necessario fare clic sull'icona **Aggiorna** () per aggiornare la tabella.
- Verificare che nessun processo sia attualmente in esecuzione sul server di destinazione. Se sono in esecuzione dei processi, il processo di aggiornamento viene messo in coda fino al completamento di tutti gli altri processi. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio → Processi**.
- Accertarsi che il repository degli aggiornamenti firmware contenga i pacchetti del firmware che si intende distribuire. In caso contrario, aggiornare il catalogo prodotti e scaricare gli aggiornamenti firmware appropriati (vedere Aggiornamento del catalogo prodotti e Download degli aggiornamenti firmware).

  Nota: Quando XClarity Administrator viene installato per la prima volta, il catalogo prodotti e il repository sono vuoti.

  Se si desidera installare il firmware prerequisito, assicurarsi che anch'esso sia stato scaricato nel repository.

  In alcuni casi, potrebbero essere necessarie più versioni per aggiornare il firmware e tutte le versioni devono essere scaricate nel repository. Ad esempio, per aggiornare lo switch scalabile IBM FC5022 SAN dalla versione 7.4.0a alla versione 8.2.0a, è necessario installare prima le versioni 8.0.1-pha e 8.1.1 e quindi la versione 8.2.0a. Per aggiornare lo switch alla versione 8.2.0a, tutte e tre le versioni devono essere state scaricate nel repository.
- In genere, per attivare gli aggiornamenti firmware occorre riavviare i dispositivi. Se si sceglie di riavviare il dispositivo durante il processo di aggiornamento (*attivazione immediata*), accertarsi che tutti i carichi di lavoro in esecuzione siano stati arrestati oppure, se si sta lavorando in un ambiente virtualizzato, siano stati spostati su un server diverso.

Per ulteriori informazioni sull'installazione degli aggiornamenti, vedere Applicazione e attivazione degli aggiornamenti firmware.

Considerazioni sugli aggiornamenti firmware

Prima di iniziare l'aggiornamento firmware per i dispositivi gestiti mediante Lenovo XClarity Administrator, leggere le seguenti importanti considerazioni.

- Considerazioni generali
- Considerazioni CMM
- Considerazioni sul controller di gestione della scheda di base
- Considerazioni sui dispositivi ThinkSystem
- Considerazioni sui dispositivi Flex System
- Considerazioni sullo storage

Considerazioni generali

- **Livelli minimi richiesti per il firmware.**

  Verificare che il firmware installato su ciascun dispositivo gestito sia aggiornato al livello minimo richiesto prima di utilizzare XClarity Administrator per aggiornare il firmware su tali dispositivi. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.

  Nota: Per informazioni sul supporto di dispositivi I/O e limitazioni conosciute, vedere Supporto XClarity Administrator - Pagina Web sulla compatibilità.

- **Aggiornare tutti i componenti al livello incluso nel repository degli aggiornamenti firmware.**

  Poiché gli aggiornamenti firmware per i componenti Flex System sono testati e rilasciati insieme, si consiglia di mantenere lo stesso livello di firmware su tutti i componenti in uno chassis di Flex System. Pertanto, è importante aggiornare il firmware su tutti i componenti dello chassis nella stessa finestra di manutenzione. XClarity Administrator applica automaticamente gli aggiornamenti selezionati nella sequenza corretta.

- **I driver LXPM Linux e LXPM Windows non sono inclusi nel download degli UXSP**

  Lenovo XClarity Provisioning Manager (LXPM) I driver Linux e Windows non sono inclusi in UpdateXpress System Packs (UXSPs). Per applicare questi pacchetti di aggiornamento ai dispositivi, scaricare i pacchetti del repository degli aggiornamenti firmware più recenti oppure scaricare manualmente i singoli pacchetti e creare un criterio di conformità del firmware per includere tali pacchetti.

- **Alcuni aggiornamenti firmware dipendono dal codice in funzione di un livello minimo del driver di dispositivo.**

  Prima di applicare gli aggiornamenti firmware di adattatore e I/O su un server, potrebbe essere necessario aggiornare un driver di dispositivo a un livello minimo. Gli aggiornamenti firmware in genere non dipendono da livelli specifici dei driver di dispositivo. Fare riferimento al file Readme dell'aggiornamento firmware per tali co-dipendenze e aggiornare i driver di dispositivo nel sistema operativo prima di aggiornare il firmware. XClarity Administrator non aggiorna i driver di dispositivo nel sistema operativo.

- **Riavviare XClarity Administrator prima di aggiornare il firmware**

  Se i tentativi precedenti di aggiornare il firmware non riescono, riavviare XClarity Administrator prima di aggiornare il firmware. Il riavvio del server di gestione garantisce che l'account riservato di sistema utilizzato per aggiornare il firmware venga sincronizzato sui dispositivi gestiti.

- **Gli aggiornamenti firmware determinano un'interruzione dell'attività e richiedono l'inattività dei carichi di lavoro sui dispositivi.**

L'esecuzione degli aggiornamenti firmware sui dispositivi gestiti determina un'interruzione dell'attività se si sceglie di aggiornare immediatamente l'aggiornamento. È necessario disattivare i dispositivi prima di aggiornare il firmware mediante la procedura di attivazione immediata.

Quando si aggiorna il firmware sui server, questi vengono arrestati e spostati in un sistema operativo di manutenzione per aggiornare i driver di dispositivo per adattatori, unità disco e unità SSD.

Switch Flex in uno specifico chassis vengono aggiornati in sequenza e riavviati durante il processo di aggiornamento firmware. L'implementazione di percorsi dati ridondanti limita il problema dell'interruzione dell'attività, ma potrebbe comunque verificarsi una breve interruzione nella connettività di rete durante l'aggiornamento firmware.

- **Non utilizzare XClarity Administrator per aggiornare il firmware sul server sul quale è in esecuzione XClarity Administrator.**

  Se XClarity Administrator viene eseguito su un host hypervisor in esecuzione su un server che sta gestendo, non utilizzare XClarity Administrator per aggiornare il firmware su quel server. Quando gli aggiornamenti firmware vengono applicati con attivazione immediata, XClarity Administrator forza il riavvio del server di destinazione, determinando di conseguenza anche il riavvio dell'host hypervisor e di XClarity Administrator. Se gli aggiornamenti vengono applicati con attivazione posticipata, solo parte del firmware viene applicata finché il sistema di destinazione non viene riavviato

Considerazioni CMM

- **Riposizionare virtualmente i CMM prima di aggiornare il firmware.**

  Se si stanno aggiornando CMM in cui da oltre tre settimane è in esecuzione una release stack del livello di firmware compresa tra 1.3.2.1 2PET12K e 2PET12Q e che presentano una configurazione a doppio CMM, è necessario riposizionare sia i CMM primari che quelli in standby prima di procedere all'aggiornamento del firmware (vedere Riposizionamento virtuale di un modulo CMM).

Considerazioni sul controller di gestione della scheda di base

- **Livelli minimi BMC richiesti per lo stato "Attivazione in sospeso"**

  Per visualizzare lo stato dell'attivazione in sospeso, è necessario installare la seguente versione del firmware sul controller di gestione della scheda di base primario del server.
  - **IMM2**: TCOO46F, TCOO46E o versioni successive (a seconda della piattaforma)
  - **XCC**: CDI328M, PSI316N, TEI334I o versioni successive (a seconda della piattaforma)

- **Aggiornamenti applicati al controller di gestione primario e alle partizioni del firmware UEFI.**

  Gli aggiornamenti di Baseboard Management Controller (BMC) e UEFI possono essere applicati alle partizioni firmware primaria e di backup per il controller di gestione e UEFI in modo indipendente.

  È anche possibile applicare gli aggiornamenti di controller di gestione e di UEFI solo alle partizioni firmware primarie sul server. Per impostazione predefinita, il controller di gestione è configurato per sincronizzare il controller di gestione di backup con la partizione del controller di gestione primario dopo aver verificato che il controller di gestione primario viene eseguito correttamente e che il nuovo livello è pronto per essere promosso a backup. Tuttavia, il controller di gestione non è configurato per sincronizzare la partizione di backup di UEFI per impostazione predefinita. Prendere in esame una delle seguenti opzioni sul controller di gestione:

  - Abilitare la sincronizzazione automatica della partizione di backup di UEFI.

    Ciò garantisce che entrambe le partizioni primaria e di backup eseguano lo stesso livello di firmware e che il firmware UEFI di backup sia compatibile con il firmware del controller di gestione.

  - Disabilitare la sincronizzazione automatica della partizione di backup del controller di gestione.

Pur trattandosi di un'operazione non consigliata, permette di acquisire il controllo completo sui livelli di firmware per il controller di gestione e UEFI. Tuttavia, è necessario aggiornare manualmente il controller di gestione e il firmware UEFI per entrambe le partizioni.

Utilizzare i criteri di conformità del firmware per determinare quali aggiornamenti vengono applicati a ciascun dispositivo. Per ulteriori informazioni sui criteri di conformità del firmware, vedere Creazione e assegnazione di criteri di conformità del firmware.

Nota: Se il controller di gestione e UEFI sono configurati per eseguire automaticamente la sincronizzazione del firmware di backup dal backup primario, non è necessario per XClarity Administrator aggiornare i banchi di backup. In tale caso, è possibile cancellare gli aggiornamenti dei banchi di backup quando si applicano gli aggiornamenti a un server oppure si rimuovono i banchi di backup dai criteri di conformità del firmware.

- **Possibilità di errore del sistema VMware vSphere ESXi (schermata diagnostica porpora dell'host) quando un controller di gestione viene reimpostato.**

  Se si sta eseguendo VMware vSphere ESXi su un qualsiasi server, assicurarsi che siano installati i livelli minimi di VMware ESXi seguenti prima di aggiornare il firmware sul server:

  – Se si sta eseguendo VMware vSphere ESXi 5.0, installare un livello minimo 5.0u2 (aggiornamento 2)
  – Se si sta eseguendo VMware vSphere ESXi 5.1, installare un livello minimo 5.1u1 (aggiornamento 1)

  Se questi livelli minimi non sono installati, potrebbe verificarsi un errore di sistema di VMware vSphere ESXi (schermata diagnostica porpora dell'host) ogni volta che il controller di gestione viene reimpostato o anche quando il firmware del controller di gestione viene applicato e attivato.

  Nota: Questo problema non interessa ESXi v5.5.

Considerazioni sui dispositivi ThinkSystem

- **Per i server ThinkSystem SE350 in cui è in esecuzione una versione firmware di XCC precedente alla 20A, l'accesso IPMI su KCS deve essere abilitato manualmente nel controller di gestione della scheda di base per garantire che il controller di gestione possa comunicare con XClarity Administrator.**

  Per i server ThinkSystem SE350, IPMI su KCS è disabilitato per impostazione predefinita. Per i server ThinkSystem SE350 in cui è in esecuzione la versione firmware 20A di XCC o successiva, XClarity Administrator abilita automaticamente IMPI su KCS durante un aggiornamento firmware e lo disabilita una volta completato l'aggiornamento. Tuttavia, per i server ThinkSystem SE350 che eseguono la versione firmware XCC precedente alla 20A, è necessario abilitare manualmente questa opzione dall'interfaccia utente di Lenovo XClarity Controller, facendo clic su **Configurazione BMC → Sicurezza → Accesso IPMI su KCS**.

- Per i server ThinkSystem SR635 e SR655, si applicano le seguenti limitazioni.

  – È supportata solo l'attivazione immediata. L'attivazione ritardata e l'attivazione con priorità non sono supportate.
  – Per XClarity Administrator v3.1.1 e versioni successive, è possibile utilizzare la funzione di aggiornamento in bundle per aggiornare tutti i componenti dei server ThinkSystem SR635 e SR655, inclusi controller di gestione della scheda di base, UEFI, unità disco e opzioni I/O.

    Attenzione: I dispositivi selezionati verranno spenti prima di avviare il processo di aggiornamento. Verificare che qualsiasi carico di lavoro in esecuzione venga interrotto oppure, se si lavora in un ambiente virtualizzato, venga spostato su un server differente. Se sono in esecuzione dei processi, il processo di aggiornamento viene messo in coda fino al completamento di tutti gli altri processi. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio → Processi**.

    Nota:

- L'applicazione degli aggiornamenti firmware in bundle è supportata solo per i server ThinkSystem SR635 e SR655.
- L'applicazione di aggiornamenti firmware in bundle è supportata solo per l'indirizzo IPv4. Gli indirizzi IPv6 non sono supportati.
- Verificare che ciascun dispositivo di destinazione sia stato avviato nel sistema operativo almeno una volta per recuperare le informazioni complete dell'inventario.
- Per utilizzare la funzione di aggiornamento in bundle è richiesto il firmware del controller di gestione della scheda di base v2.94 o versione successiva.
- Vengono utilizzati solo gli aggiornamenti firmware dei pacchetti del repository o i singoli aggiornamenti firmware. I pacchetti UpdateXpress System Packs (UXSPs) non sono supportati.
- Solo gli aggiornamenti firmware scaricati vengono applicati. Aggiornare il catalogo prodotti e scaricare gli aggiornamenti firmware appropriati (vedere Aggiornamento del catalogo prodotti e Download degli aggiornamenti firmware).

  Nota: Quando XClarity Administrator viene installato per la prima volta, il catalogo prodotti e il repository sono vuoti.
- Il controllo di conformità è supportato solo per il controller di gestione della scheda di base e UEFI nei server ThinkSystem SR635 e SR655. XClarity Administrator tenta comunque di applicare gli aggiornamenti firmware a tutti i componenti hardware disponibili.
- Gli aggiornamenti vengono applicati in base ai criteri di conformità del firmware assegnati. Non è possibile scegliere di aggiornare un sottoinsieme di componenti.
- XClarity Administrator v3.2 o versione successiva è richiesto per applicare gli aggiornamenti firmware per Lenovo XClarity Provisioning Manager (LXPM), i driver Windows LXPM o i driver Linux LXPM ai server ThinkSystem SR635 e SR655.
- Gli aggiornamenti del controller di gestione della scheda di base e UEFI vengono ignorati se la versione attualmente installata è superiore ai criteri di conformità assegnati.
- I criteri di conformità del firmware devono essere creati e assegnati ai dispositivi ai quali si desidera applicare gli aggiornamenti firmware. Per ulteriori informazioni, vedere Creazione e assegnazione di criteri di conformità del firmware.
- I dispositivi selezionati verranno spenti prima di avviare il processo di aggiornamento. Verificare che qualsiasi carico di lavoro in esecuzione venga interrotto oppure, se si lavora in un ambiente virtualizzato, venga spostato su un server differente.

È anche possibile utilizzare la funzione di aggiornamento tradizionale per applicare gli aggiornamenti firmware solo al controller di gestione della scheda di base e UEFI.

- Per XClarity Administrator v3.0:
  - I dati di gestione non vengono aggiornati correttamente durante l'aggiornamento del firmware da 20A a 20B o 20C. Per risolvere il problema, annullare la gestione, quindi gestire nuovamente il dispositivo oppure riavviare il sistema XClarity Administrator.
  - Il downgrade degli aggiornamenti firmware non è supportato.

- **Gli aggiornamenti firmware non sono supportati sui server ThinkSystem che utilizzano DHCPv6 o gli indirizzi IPv6 assegnati staticamente**

  Quando si utilizza l'indirizzamento IPv6 sui server ThinkSystem, gli aggiornamenti firmware sono supportati soltanto sugli indirizzi IPv6 Link-Local Address (LLA) e stateless.

- **Quando si aggiorna il firmware alla versione 20D, è necessario aggiornare insieme UEFI e XCC.**

  UEFI e Lenovo XClarity Controller (XCC) devono essere aggiornati insieme per la versione 20D. L'aggiornamento di XCC e non di UEFI, e viceversa, causerà problemi.

Considerazioni sui dispositivi Flex System

- **Accertarsi che gli switch Flex aggiornati siano accesi.**
- **Selezionare Attivazione immediata quando si aggiornano i nodi di elaborazione con livelli di firmware del controller di gestione precedenti a Flex System 1.3.2.**

  Quando si applica Flex System 1.3.2, release del ciclo di vita del secondo trimestre, a un nodo di elaborazione, è necessario scegliere l'*attivazione immediata* per aggiornare il nodo di elaborazione. L'attivazione immediata forza il riavvio del nodo di elaborazione durante il processo di aggiornamento.
- **Switch Flex devono essere configurati con un indirizzo IP raggiungibile da XClarity Administrator.**

  Allo Switch Flex di destinazione deve essere assegnato un indirizzo IP che può comunicare con XClarity Administrator in modo che XClarity Administrator possa scaricare e applicare l'aggiornamento firmware.
- **Supporto dell'aggiornamento sui complessi scalabili, quali i nodi x480 X6 e x880 X6.**

  Il supporto degli aggiornamenti sui nodi scalabili, come i nodi di elaborazione x480 X6 e x880 X6 di Flex System è limitato alle configurazioni in cui il complesso è configurato come una *partizione singola* che include tutti i nodi di elaborazione che fanno parte del complesso multinodo. Non è possibile utilizzare XClarity Administrator per aggiornare un complesso costituito da più partizioni.

  Se si assegnano dei criteri di conformità del firmware a una partizione che include più server in un complesso scalabile (come Nodi di elaborazione Flex System x480 X6 e Nodi di elaborazione Flex System x880 X6), XClarity Administrator aggiorna il firmware su tutti i controller di gestione e gli UEFI per ciascun server nella partizione per impostazione predefinita. Tuttavia, se si seleziona un sottoserie di componenti all'interno della partizione, XClarity Administrator aggiorna il firmware solo sui componenti selezionati nella partizione.
- **Prima di aggiornare il CMM2 alla v1.30 (1AON06C) o successiva, è necessario che gli switch Flex eseguano la versione di livello 3 di Enhanced Configuration and Management (EHCM L3)**

  Il CMM2 e gli switch Flex comunicano mediante il protocollo EHCM. Questo protocollo è necessario XClarity Administrator per aggiornare gli switch Flex. Quando si aggiorna un CMM2 alla v1.30 (1AON06C) o successiva, XClarity Administrator verifica che gli switch Flex stiano eseguendo EHCM L3; in caso contrario, l'aggiornamento di CMM viene annullato e viene visualizzata un'avvertenza per indicare che occorre prima aggiornare gli switch Flex a una versione che supporti EHCM-L3. È possibile ignorare questa verifica selezionando **Tentativo di aggiornamento di componenti già conformi** quando si aggiorna il firmware del CMM.

  Attenzione: Attualmente non sono disponibili versioni firmware per gli switch Ethernet Flex System EN6131 e gli switch InfiniBand IB6131 in grado di supportare EHCM L3. Ciò significa che dopo aver aggiornato il firmware del CMM2 alla v1.30 (1AON06C) o successiva, non è più possibile utilizzare XClarity Administrator per aggiornare tali switch. La soluzione alternativa consiste nell'utilizzare l'interfaccia Web o l'interfaccia della riga di comando del controller di gestione affinché lo chassis aggiorni lo switch.

Switch Flex System	Versione	Data di rilascio
CN4093	7.8.4.0	Giugno 2014
EN4023	6.0.0	Aprile 2015
EN4093	7.8.4.0	Giugno 2014
EN4093R	7.8.4.0	Giugno 2014
EN6132	Non disponibile	Non disponibile
FC3171	9.1.3.02.00	Giugno 2014
FC5022	7.4.0b1	Marzo 2016

Switch Flex System	Versione	Data di rilascio
IB6132	Non disponibile	Non disponibile
SI4091	7.8.4.0	Giugno 2014
SI4093	7.8.4.0	Giugno 2014

Nota: Lo switch scalabile Ethernet EN2092 1 Gb non richiede EHCM L3 e non è soggetto a questa limitazione.

Considerazioni sullo storage

- **Considerazioni sui dispositivi di storage ThinkSystem della serie DM**

  Per aggiornare il firmware dei dispositivi di storage ThinkSystem della serie DM, è necessario che siano in esecuzione i dispositivi v9.7 o versione successiva.

  Il downgrade è supportato solo per le versioni secondarie. Ad esempio, è possibile eseguire il downgrade da 9,7P11 a 9,7P9; tuttavia, non è possibile eseguire il downgrade da 9,8 a 9,7.

  Per scaricare il firmware per i dispositivi di storage ThinkSystem della serie DM:

  - Uno o più dispositivi di storage ThinkSystem della serie DM devono essere gestiti da XClarity Administrator.
  - Ogni dispositivo di storage ThinkSystem della serie DM deve essere autorizzato per l'assistenza e il supporto hardware.
  - Nella pagina Aggiornamenti firmware: Repository è necessario specificare il paese in cui si trovano i dispositivi di storage ThinkSystem della serie DM. Solo il firmware crittografato può essere scaricato per i dispositivi nei seguenti paesi: Armenia, Bielorussia, Cina, Corea del Nord, Cuba, Iran, Kazakistan, Kirghizistan, Russia, Siria, Sudan.

- **Le unità disco devono trovarsi nello stato JBOD, Online, Pronto o Non configurato (valido).**

  Per aggiornare il firmware sulle unità disco, lo stato RAID deve essere JBOD, Online, Pronto o Non configurato (valido). Gli altri stati non sono supportati. Per determinare lo stato RAID di un'unità disco, accedere alla pagina Inventario per il dispositivo, espandere la sezione **Unità** e controllare la colonna **Stato RAID** per tale unità disco (vedere Visualizzazione dei dettagli di un server gestito).

- **La versione firmware non rileva le unità disco e le unità SSD.**

  XClarity Administrator rileva solo la versione firmware installata ed esegue un controllo di conformità per le unità disco e le unità SSD collegate a un adattatore MegaRAID o NVME. Le altre unità potrebbero avere un livello di firmware non supportato oppure potrebbero non supportare la segnalazione della versione firmware. Tuttavia, gli aggiornamenti firmware vengono applicati a tali unità una volta selezionati.

- **Il firmware NVMe viene applicato anche se non è identificato con un componente di destinazione.**

  Nella pagina Applica/Attiva, viene elencata la versione firmware NVMe per le unità SSD. Dal momento che non viene identificato alcun aggiornamento firmware di destinazione per i dispositivi NVMe rilevati, viene visualizzato un messaggio di avvertenza quando si tenta di aggiornare il sistema di destinazione. Tuttavia, l'aggiornamento delle unità disco fisso/SSD viene applicata anche se non è identificato con un componente di destinazione, in modo che il firmware NVMe sia costantemente aggiornato.

- **L'applicazione del pacchetto di aggiornamento ServeRAID M5115 PSoC3 da XClarity Administrator richiede che il livello minimo installato sia 68.**

  L'aggiornamento ServeRAID M5115 PSoC3 (Programmable System-on-Chip) da una versione precedente alla 68 deve essere effettuato in maniera controllata.

  Suggerimento: è possibile visualizzare la versione del codice per ServeRAID M5115 PSoC3 effettuando il login all'interfaccia Web CMM e selezionando la scheda **Firmware** per il nodo di elaborazione di

destinazione. Quindi, selezionare la scheda di espansione per l'adattatore di ServeRAID M5115. La versione del codice PSoc3 è il tipo di firmware GENERIC.

Per le versioni installate precedenti alla 68, non è possibile eseguire l'aggiornamento mediante XClarity Administrator. È invece necessario eseguire le seguenti operazioni dall'interfaccia Web o dall'interfaccia della riga di comando (CLI) di Chassis Management Module (CMM):

- **Utilizzo dell'interfaccia Web CMM:**
  1. Effettuare il login all'interfaccia Web CMM (Chassis Management Module).
  2. Nel menu principale, fare clic su **Assistenza e supporto → Avanzata**.
  3. Fare clic sulla scheda **Ripristino servizio**.
  4. Selezionare il nodo di elaborazione appropriato facendo clic sul relativo pulsante di scelta.
  5. Dall'elenco a discesa **Reimposta**, fare clic su **Riposizionamento virtuale**.
  6. Fare clic su **OK** per confermare.
- **Utilizzo dell'interfaccia della riga di comando CMM**:
  - Effettuare il login all'interfaccia Secure Shell (SSH) del CMM.
  - Immettere il seguente comando per eseguire un riposizionamento virtuale:
    ```
    'service -vr -T blade[x]
    ```
    dove *x* è il numero del vano del nodo di elaborazione da riposizionare.

Una volta che il sistema viene riacceso, avviare il sistema operativo e aggiornare ServeRAID M5115 PSoC3 utilizzando il pacchetto di aggiornamento incorporato estratto. Completare le seguenti operazioni per estrarre il pacchetto incorporato.

- **Utilizzo di Microsoft Windows:**

  Aprire il pacchetto di aggiornamento (lnvgy_fw_psoc3_m5115-70_windows_32-64.exe) e selezionare Estrai su disco fisso. Selezionare quindi il percorso in cui il pacchetto incorporato deve essere estratto.
- **Utilizzo di Linux:**

  Eseguire il seguente comando:
  ```
  lnvgy_fw_psoc3_m5115-70_linux_32-64.bin -x
  ```
  dove *x* è la posizione in cui deve essere estratto il pacchetto incorporato.

Gestione del repository degli aggiornamenti firmware

Il *repository degli aggiornamenti firmware* contiene un catalogo di aggiornamenti disponibili e i pacchetti di aggiornamento applicabili ai dispositivi gestiti.

Informazioni su questa attività

Il *catalogo* contiene informazioni relative agli aggiornamenti firmware attualmente disponibili per tutti i dispositivi supportati da XClarity Administrator. Il catalogo organizza gli aggiornamenti firmware per tipo di dispositivo. Quando si aggiorna il catalogo, XClarity Administrator recupera le informazioni sugli ultimi aggiornamenti firmware disponibili dal sito Web di Lenovo (inclusi i file metadata.xml o .json e readme.txt) e le archivia nel repository degli aggiornamenti firmware. Il file di payload (.exe) non è stato scaricato. Per ulteriori informazioni sull'aggiornamento del catalogo, vedere Aggiornamento del catalogo prodotti.

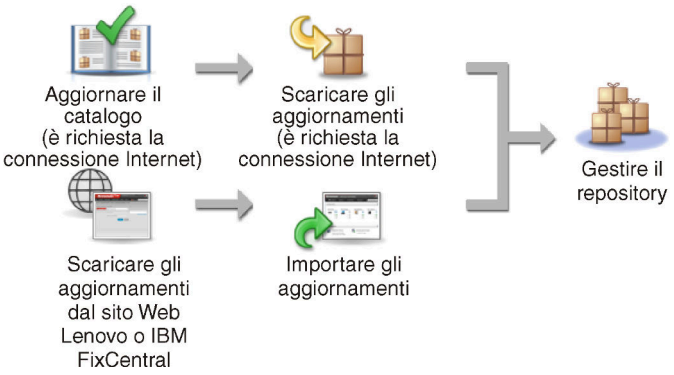
Se sono disponibili nuovi aggiornamenti firmware, è necessario scaricare i pacchetti di aggiornamento prima di aggiornare il firmware sui dispositivi gestiti. L'aggiornamento del catalogo non include il download automatico dei pacchetti di aggiornamento. La tabella **Catalogo prodotti** nella pagina Repository aggiornamenti firmware identifica i pacchetti di aggiornamento scaricati e quelli disponibili per il download.

È possibile scaricare gli aggiornamenti firmware in diversi modi:

- **Pacchetti del repository degli aggiornamenti firmware**. I pacchetti del repository contengono i più recenti aggiornamenti firmware disponibili per tutti i dispositivi supportati e i criteri di conformità del firmware predefiniti. Questi pacchetti del repository vengono importati e successivamente applicati attraverso la pagina Aggiorna server di gestione.
- **UpdateXpress System Packs (UXSPs)**. I pacchetti UXSP contengono i più recenti aggiornamenti disponibili dei driver di dispositivo e dei firmware, organizzati per sistema operativo. Quando si scaricano i pacchetti UXSP dalla pagina Aggiornamenti firmware: Repository, solo gli aggiornamenti firmware vengono scaricati e memorizzati nel repository. Gli aggiornamenti dei driver di dispositivo non sono inclusi.

  Nota: Per i server con XCC2, questi pacchetti vengono definiti *bundle* di firmware.
- **Aggiornamenti firmware individuali**. È possibile scaricare i singoli pacchetti di aggiornamento firmware individuali, in base alla versione elencata nel catalogo.

XClarity Administrator deve essere collegato a Internet per aggiornare il catalogo e scaricare gli aggiornamenti firmware. Se non è collegato a Internet, è possibile scaricare manualmente i file in una workstation che ha accesso alla rete nell'host XClarity Administrator, tramite un browser Web e quindi importare i file nel repository degli aggiornamenti firmware.



Quando si importano manualmente gli aggiornamenti firmware in XClarity Administrator, è necessario includere i seguenti file: payload (immagine e MIB), metadati, cronologia delle modifiche e readme. Ad esempio:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Attenzione:

- Importare solo questi file obbligatori. Non importare altri file che potrebbero essere disponibili nei siti Web di download del firmware.
- Se non si include il file XML nel pacchetto di aggiornamento, l'aggiornamento non viene importato.
- Se non si includono tutti i file richiesti associati all'aggiornamento, il repository contrassegna l'aggiornamento come non scaricato, ad indicare che è stato parzialmente importato. È quindi possibile importare i file mancanti selezionandoli e importandoli.
- Gli aggiornamenti firmware principali (come il controller di gestione, UEFI e pDSA) sono indipendenti del sistema operativo. I pacchetti di aggiornamento firmware per i sistemi operativi RHEL 6 o SLES 11 sono utilizzati per aggiornare i nodi di elaborazione e i server rack. Per ulteriori informazioni sui pacchetti di aggiornamento firmware da utilizzare per i server gestiti, vedere Download degli aggiornamenti firmware.

Una volta scaricati gli aggiornamenti firmware nel repository, vengono fornite informazioni su ciascun aggiornamento, inclusi la data di rilascio, la dimensione, l'utilizzo dei criteri e la gravità. La gravità indica l'impatto e la necessità di applicare gli aggiornamenti utili a valutare come il proprio ambiente potrebbe essere interessato.

- **Release iniziale**. Questa è la prima release del firmware.
- **Critico**. La release del firmware contiene correzioni urgenti per problemi relativi al danneggiamento dei dati, alla sicurezza o alla stabilità.
- **Consigliato**. La release del firmware contiene correzioni significative per i problemi che potrebbero verificarsi.
- **Non critico**. La release del firmware contiene correzioni minori, miglioramenti delle prestazioni e modifiche testuali.

Nota:

- La gravità è relativa alla versione dell'aggiornamento rilasciata in precedenza. Ad esempio, se il firmware installato è v1.01 e l'aggiornamento v1.02 è Critico mentre l'aggiornamento v1.03 è Consigliato, ciò significa che l'aggiornamento da 1.02 a 1.03 è consigliato, ma aggiornamento da v1.01 a v1.03 è critico poiché è cumulativo (v1.03 include le correzioni ai problemi critici disponibili in v1.02).
- Casi speciali potrebbero verificarsi se un aggiornamento è solo critico o consigliato per un tipo di macchina o un sistema operativo specifico. Fare riferimento alle note di rilascio per ulteriori informazioni.

Procedura

Per visualizzare gli aggiornamenti firmware disponibili nel catalogo prodotti, completare le seguenti operazioni.

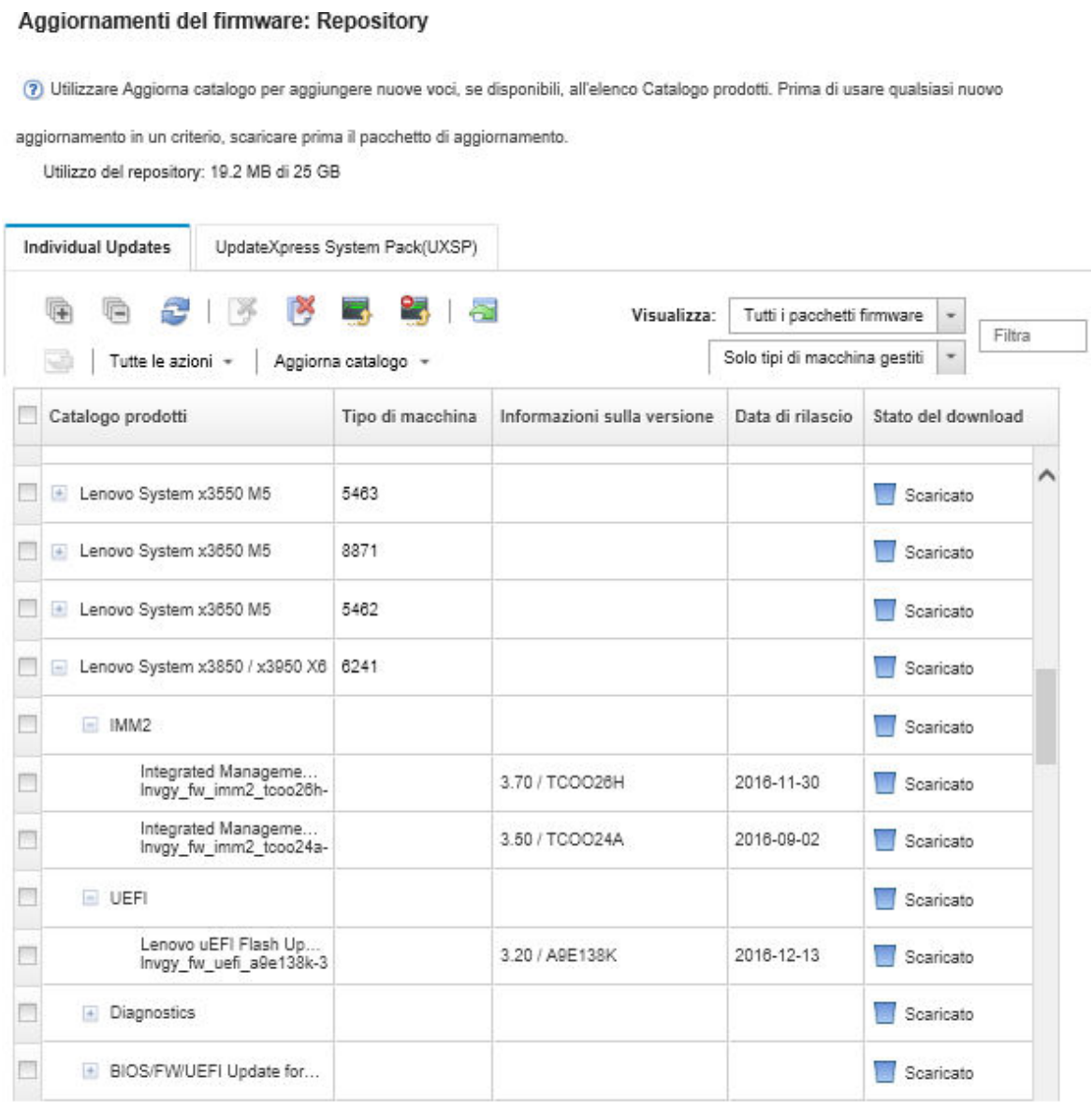
Passo 1. Dalla barra di menu di XClarity Administrator, fare clic su **Provisioning → Repository**. Viene visualizzata la pagina Repository aggiornamenti firmware contenente un elenco di pacchetti di aggiornamento firmware disponibili, organizzato per tipo di dispositivo.

Passo 2. Fare clic sulla scheda **Aggiornamenti individuali** per visualizzare le informazioni disponibili sui pacchetti di aggiornamento firmware disponibili oppure fare clic sulla scheda **UpdateXpress System Packs (UXSPs)** per visualizzare le informazioni disponibili sui pacchetti UXSP.

Passo 3. Espandere un dispositivo e i relativi componenti per visualizzare l'elenco dei pacchetti di aggiornamento e degli aggiornamenti firmware per tale dispositivo.

È possibile ordinare le colonne della tabella e fare clic sull'icona **Espandi tutto** () e **Comprimi tutto** () per rendere più semplice trovare gli aggiornamenti firmware specifici. Inoltre, è possibile filtrare l'elenco dei dispositivi visualizzati e degli aggiornamenti firmware, selezionando un'opzione nel menu **Mostra** per elencare solo gli aggiornamenti firmware di un periodo specifico per tutti i tipi di server o solo per tipi di server gestiti. In alternativa, immettere il testo nel campo **Filtro**. Nota: se si cercano dispositivi specifici, vengono elencati solo i dispositivi; gli aggiornamenti firmware non vengono elencati sotto il nome del dispositivo.

Nota: Per i server, i pacchetti di aggiornamento specifici sono disponibili in base al tipo di server. Ad esempio, se si espande un server, come Nodo di elaborazione Flex System x240, vengono visualizzati i pacchetti di aggiornamento disponibili specificamente per tale nodo di elaborazione.



Risultati

Da questa pagina, è possibile eseguire le seguenti azioni:

- Aggiornare questa pagina con le informazioni di aggiornamento firmware correnti nel catalogo facendo clic sull'icona **Aggiorna** ( ).
- Recuperare le informazioni più recenti sugli aggiornamenti disponibili facendo clic su **Aggiorna catalogo**. Il recupero di queste informazioni potrebbe richiedere alcuni minuti. Per ulteriori informazioni, vedere Aggiornamento del catalogo prodotti.
- Aggiungere gli aggiornamenti firmware al repository selezionando uno o più pacchetti di aggiornamento o aggiornamenti nel catalogo prodotti e facendo quindi clic sull'icona **Scarica** ( ). Quando gli aggiornamenti firmware sono stati scaricati e aggiunti al repository, lo stato viene modificato in "Scaricato".

Nota: XClarity Administrator deve essere collegato a Internet per acquisire gli aggiornamenti mediante l'interfaccia utente di XClarity Administrator. Se non è collegato a Internet, è possibile importare gli aggiornamenti precedentemente scaricati.

Per ulteriori informazioni sul download degli aggiornamenti, vedere Download degli aggiornamenti firmware.

- Importare gli aggiornamenti firmware scaricati manualmente in una workstation con accesso di rete a XClarity Administrator selezionando uno o più aggiornamenti e facendo quindi clic sull'icona **Importa** ( ).Per ulteriori informazioni sull'importazione degli aggiornamenti, vedere Download degli aggiornamenti firmware.
- Arrestare i download dei firmware attualmente in corso selezionando uno o più aggiornamenti e facendo quindi clic sull'icona **Annulla download** ( ).L'annullamento dei download annulla *tutti* i download dei firmware in corso. È possibile monitorare l'avanzamento dettagliato e arrestare uno specifico download di firmware dal log dei processi (vedere Monitoraggio dei processi).
- Eliminare i pacchetti di aggiornamento o i singoli aggiornamenti dal repository (vedere Eliminazione degli aggiornamenti firmware).
- Esportare gli aggiornamenti presenti nel repository degli aggiornamenti firmware in un sistema locale (vedere Esportazione e importazione degli aggiornamenti firmware).

Utilizzo di un repository remoto per gli aggiornamenti firmware

Per impostazione predefinita, Lenovo XClarity Administrator utilizza un repository (interno) locale per gli aggiornamenti firmware disponibili. È possibile liberare lo spazio su disco disponibile nel repository locale XClarity Administrator utilizzando una condivisione remota montata su SSH File System (SSHTF) come repository remoto. È quindi possibile utilizzare i file di aggiornamento firmware direttamente dal repository remoto per mantenere la conformità del firmware sui dispositivi.

Prima di iniziare

Nella condivisione remota possono essere memorizzati solo gli aggiornamenti firmware. Gli aggiornamenti e i driver di dispositivo di Windows e XClarity Administrator possono essere memorizzati solo nel repository degli aggiornamenti locali.

Verificare che il servizio SFTP sulla porta 22 sia aperto sul server di condivisione remota. I controller di gestione della scheda di base devono avere accesso a questa porta.

La condivisione remota viene utilizzata come server SFTP quando viene usata come repository firmware. Accertarsi di non disabilitare SFTP quando si aggiorna la configurazione SSHD.

Informazioni su questa attività

Quando si modifica la posizione del repository degli aggiornamenti firmware, è possibile scegliere di copiare tutti gli aggiornamenti firmware dal repository originale al nuovo repository.

I file di aggiornamento firmware nel repository originale *non vengono* puliti automaticamente dopo il cambio di posizione.

Se XClarity Administrator dispone di autorizzazioni di lettura-scrittura sul repository remoto, il comportamento è identico a quando si utilizza il repository locale. Tuttavia, se XClarity Administrator dispone di autorizzazioni di sola lettura, non è possibile aggiornare il catalogo e scaricare o importare gli aggiornamenti nel repository.

Lo stesso repository remoto può essere condiviso da più istanze XClarity Administrator; tuttavia, se un'istanza XClarity Administrator modifica il repository, le altre istanze XClarity Administrator non vengono avvisate automaticamente. È necessario aggiornare il repository per ottenere i dettagli più recenti. Per aggiornare il repository, fare clic su **Tutte le azioni → Aggiorna repository** dalla pagina Aggiornamenti firmware: Repository.

Nota: Prestare attenzione quando si eliminano gli aggiornamenti firmware e gli UXSP se il repository degli aggiornamenti firmware si trova su una condivisione remota utilizzata da più istanze di XClarity Administrator.

Procedura

Per utilizzare un repository degli aggiornamenti firmware remoto, completare le seguenti operazioni.

Passo 1. Aggiungere una condivisione remota a XClarity Administrator (vedere Gestione condivisioni remote).

Passo 2. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Repository**. Viene visualizzata la pagina Repository aggiornamenti firmware.

Passo 3. Fare clic su **Tutte le azioni → Scambia posizione repository** per visualizzare la finestra di dialogo Scambia posizione repository.

Passo 4. Selezionare la condivisione remota appena creata dall'elenco a discesa **Posizione repository**.

Passo 5. Facoltativamente selezionare **Pulisci repository corrente** per eliminare i file dell'aggiornamento firmware dalla posizione del repository corrente.

Passo 6. Facoltativamente selezionare **Copia pacchetti di aggiornamento dal repository corrente nel nuovo repository** per copiare i file di aggiornamento firmware nella nuova posizione del repository prima di passare alla posizione del repository.

Per impostazione predefinita, i file di aggiornamento firmware esistenti nella nuova posizione non vengono copiati (vengono ignorati). Facoltativamente è possibile scegliere di sovrascrivere tutti i file esistenti o di sovrascrivere solo i file esistenti di dimensioni o date di modifica diverse dall'elenco a discesa **Sovrascrivi regole**.

Passo 7. Fare clic su **OK**.

Viene creato un processo per copiare i pacchetti di aggiornamento firmware nel nuovo repository. Per monitorare l'avanzamento del processo, fare clic su **Monitoraggio → Processi** dalla barra dei menu di XClarity Administrator.

Aggiornamento del catalogo prodotti

Il catalogo prodotti contiene informazioni relative agli aggiornamenti firmware attualmente disponibili per tutti i dispositivi supportati da Lenovo XClarity Administrator, inclusi chassis, server e Switch Flex.

Prima di iniziare

È necessaria una connessione Internet per aggiornare il catalogo prodotti.

Il completamento dell'aggiornamento del catalogo potrebbe richiedere diversi minuti.

Informazioni su questa attività

Quando si aggiorna il catalogo, XClarity Administrator recupera le informazioni sugli ultimi aggiornamenti firmware disponibili dal Sito Web del supporto per Lenovo XClarity e le memorizza nel repository degli aggiornamenti firmware.

L'aggiornamento del catalogo aggiunge solo informazioni sugli aggiornamenti firmware disponibili al repository. Non scarica i pacchetti di aggiornamento. È necessario scaricare gli aggiornamenti firmware per rendere gli aggiornamenti disponibili per l'installazione. Per ulteriori informazioni sul download degli aggiornamenti, vedere Download degli aggiornamenti firmware.

Procedura

Per aggiornare il catalogo prodotti, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Repository**. Viene visualizzata la pagina Repository aggiornamenti firmware.

Passo 2. Fare clic sulla scheda **Aggiornamenti individuali** per recuperare le informazioni sui pacchetti di aggiornamento firmware individuali oppure fare clic sulla scheda **UpdateXpress System Pack (UXSP)** per recuperare le informazioni sui pacchetti UXSP.

Passo 3. Fare clic su **Aggiorna catalogo**, quindi selezionare una delle seguenti opzioni per ottenere informazioni sugli ultimi aggiornamenti firmware disponibili.

- **Aggiorna elementi selezionati - Solo il più recente**. Recupera le informazioni sulla versione più aggiornata degli aggiornamenti firmware disponibili solo per i dispositivi selezionati.
- **Aggiorna tutto - Solo il più recente**. Recupera le informazioni sulla versione più aggiornata di tutti aggiornamenti firmware per tutti i dispositivi supportati.
- **Aggiorna elementi selezionati**. Recupera le informazioni su tutte le versioni degli aggiornamenti firmware disponibili solo per i dispositivi selezionati.
- **Aggiorna tutto**. Recupera le informazioni su tutte le versioni di tutti gli aggiornamenti firmware disponibili per tutti i dispositivi selezionati.

Suggerimento: è possibile aggiornare il catalogo prodotti e scaricare il firmware più recente in un solo passaggio facendo clic su **Tutte le azioni → Aggiorna e scarica la versione più recente per tutti i dispositivi gestiti** oppure selezionando **Tutte le azioni → Aggiorna e scarica la versione più recente per i dispositivi selezionati**.

Download degli aggiornamenti firmware

È possibile scaricare o importare gli aggiornamenti firmware nel repository degli aggiornamenti firmware, a seconda dell'accesso a Internet. Gli aggiornamenti firmware devono essere disponibili nel repository degli aggiornamenti firmware affinché sia possibile procedere all'aggiornamento firmware sui dispositivi di gestione.

Prima di iniziare

Verificare che tutte le porte e l'indirizzo Internet che Lenovo XClarity Administrator richiede siano disponibili prima di tentare di scaricare il firmware. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta e Firewall e server proxy nella documentazione online di XClarity Administrator.

Se un tipo di dispositivo non è elencato nel repository degli aggiornamenti firmware, è necessario gestire un dispositivo di quel tipo prima di scaricare o di importare i singoli aggiornamenti firmware per tale tipo di dispositivo.

Importante:

- Per XClarity Administrator v1.1.1 e versioni precedenti, è necessario scaricare e importare manualmente gli aggiornamenti firmware per Lenovo Hardware da Sito Web dell'Assistenza del Centro Dati Lenovo.
- XClarity Administrator non può scaricare gli aggiornamenti per gli switch RackSwitch e i dispositivi Lenovo Storage delle serie DE, DX e SS dal sito Web di Lenovo nel repository degli aggiornamenti firmware; è pertanto necessario scaricare manualmente e importare questi aggiornamenti RackSwitch e Lenovo

Storage dal sito Web di Lenovo a una workstation che ha accesso di rete nell'host XClarity Administrator oppure scaricare e applicare i *pacchetti del repository degli aggiornamenti firmware*, che contengono tutti gli aggiornamenti firmware disponibili.

- I browser Internet Explorer e Microsoft Edge hanno un limite di caricamento di 4 GB. Se il file da importare è maggiore di 4 GB, considerare la possibilità di utilizzare un altro browser Web (come Chrome o Firefox).
- Per scaricare il firmware per i dispositivi di storage ThinkSystem della serie DM:
  - Uno o più dispositivi di storage ThinkSystem della serie DM devono essere gestiti da XClarity Administrator.
  - Ogni dispositivo di storage ThinkSystem della serie DM deve essere autorizzato per l'assistenza e il supporto hardware.
  - Nella pagina Aggiornamenti firmware: Repository è necessario specificare il paese in cui si trovano i dispositivi di storage ThinkSystem della serie DM. Solo il firmware crittografato può essere scaricato per i dispositivi nei seguenti paesi: Armenia, Bielorussia, Cina, Corea del Nord, Cuba, Iran, Kazakistan, Kirghizistan, Russia, Siria, Sudan.

Informazioni su questa attività

È possibile scaricare gli aggiornamenti firmware in diversi modi:

- **Pacchetti del repository degli aggiornamenti firmware**

  I pacchetti del repository degli aggiornamenti firmware sono raccolte del firmware più recente che è disponibile contemporaneamente al rilascio di XClarity Administrator per molti dispositivi supportati, nonché criteri di conformità del firmware predefiniti. Questi pacchetti del repository vengono importati e successivamente applicati attraverso la pagina Aggiorna server di gestione. Quando si applica un pacchetto del repository degli aggiornamenti firmware, ogni pacchetto di aggiornamento viene aggiunto al repository degli aggiornamenti firmware e vengono creati automaticamente criteri di gestione del firmware per tutti i dispositivi gestibili. Questo criterio predefinito può essere copiato ma non modificato.

  Sono disponibili i seguenti pacchetti del repository.

  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i CMM e gli switch Flex System.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per tutti gli switch RackSwitch e i dispositivi Lenovo Storage.
  - **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per i server Converged serie HX, Flex System, NeXtScale e System x.
  - **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i server ThinkAgile e ThinkSystem.
  - **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i server ThinkAgile e ThinkSystem V2.
  - **lnvgy_sw_lxca_thinksystemv3repo***x-x.x.x*_**anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i server ThinkAgile e ThinkSystem V3.

  È possibile determinare se i pacchetti del repository degli aggiornamenti firmware vengono memorizzati nel repository verificando il valore della colonna **Stato download** nella pagina Aggiorna server di gestione. Questa colonna contiene i seguenti valori:

  - **Scaricato**. Il pacchetto del repository degli aggiornamenti firmware è memorizzato nel repository.
  - **Non scaricato**. Il pacchetto del repository degli aggiornamenti firmware è disponibile ma non è memorizzato nel repository.
- **UpdateXpress System Packs (UXSPs)**

Nota: Per i server con XCC2, questi pacchetti vengono definiti bundle di firmware. Il *bundle* viene utilizzato nei nomi dei pacchetti e nei nomi dei criteri predefiniti.

I pacchetti UXSP contengono i più recenti aggiornamenti disponibili dei driver di dispositivo e dei firmware, organizzati per sistema operativo. Quando si scaricano i pacchetti UXSP, XClarity Administrator scarica il pacchetto UXSP in base alla versione elencata nel catalogo e memorizza i pacchetti di aggiornamento nel repository degli aggiornamenti firmware. Quando si scarica un pacchetto UXSP, ogni aggiornamento firmware in UXSP viene aggiunto al repository degli aggiornamenti firmware ed elencato nella scheda **Aggiornamenti individuali** e vengono creati automaticamente criteri di conformità del firmware per tutti i dispositivi gestibili utilizzando i seguenti nomi. Questo criterio predefinito può essere copiato ma non modificato.

- *{uxsp-version}-{date}-{server-short-name}***-UXSP** (ad esempio, `v1.50-2017-11-22- SD530-UXSP`)
- *{uxsp-version}-{buildnumber}-{server-short-name}***-bundle** (ad esempio, `22a.0-kaj92va-SR650V3-bundle`)

Nota: Quando si scaricano o si importano i pacchetti UXSPs dalla pagina Aggiornamenti firmware: Repository, solo gli aggiornamenti firmware vengono scaricati e memorizzati nel repository. Gli aggiornamenti dei driver di dispositivo vengono ignorati. Per informazioni sul download o l'importazione dei driver di dispositivo di Windows mediante i pacchetti UXSPs, vedere Gestione del repository dei driver di dispositivo del sistema operativo.

È possibile determinare se i pacchetti UXSPs vengono archiviati nel repository degli aggiornamenti firmware nella colonna **Stato del download** nella scheda **Aggiornamenti individuali** della pagina Aggiornamenti firmware: Repository. Questa colonna contiene i seguenti valori:

- **Scaricato**. L'intero pacchetto di aggiornamento o i singoli aggiornamenti firmware vengono memorizzati nel repository.
- *x* **di** *y* **Scaricato**. Non tutti gli aggiornamenti firmware nel pacchetto di aggiornamento sono memorizzati nel repository. I numeri tra parentesi indicano il numero di aggiornamenti disponibili e il numero di aggiornamenti memorizzati, oppure l'indisponibilità di aggiornamenti per il tipo di dispositivo specifico.
- **Non scaricato**. L'intero pacchetto di aggiornamento o i singoli aggiornamenti firmware sono disponibili ma non sono memorizzati nel repository.

- **Aggiornamenti firmware individuali**

  È possibile scaricare i singoli pacchetti di aggiornamento firmware individuali. Quando si scaricano i pacchetti di aggiornamento firmware, XClarity Administrator scarica l'aggiornamento in base alla versione elencata nel catalogo e memorizza i pacchetti di aggiornamento nel repository degli aggiornamenti firmware. È possibile quindi creare i criteri di conformità del firmware utilizzando tali pacchetti di aggiornamento per ciascuno dei dispositivi gestiti.

  Nota: Gli aggiornamenti firmware principali (come il controller di gestione, UEFI e pDSA) sono indipendenti del sistema operativo. I pacchetti di aggiornamento firmware per i sistemi operativi RHEL 6 o SLES 11 sono utilizzati per aggiornare i nodi di elaborazione e i server rack. Per ulteriori informazioni sui pacchetti di aggiornamento firmware da utilizzare per i server gestiti, vedere Download degli aggiornamenti firmware.

  È possibile determinare se gli specifici *aggiornamenti firmware* vengono memorizzati nel repository degli aggiornamenti firmware verificando il valore della colonna **Stato del download** nella scheda **Aggiornamenti individuali** della pagina Aggiornamenti firmware: Repository. Questa colonna contiene i seguenti valori.

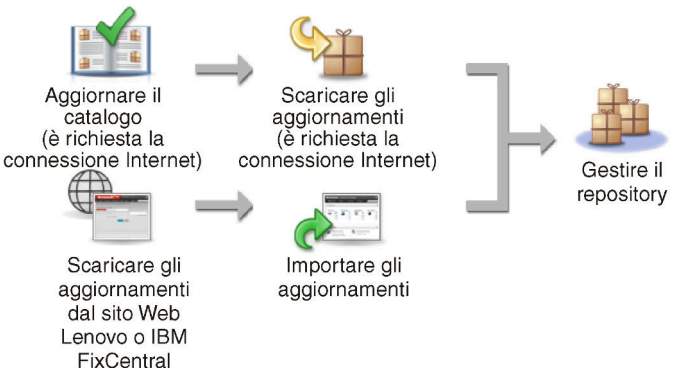
  - **Scaricato**. L'intero pacchetto di aggiornamento o i singoli aggiornamenti firmware vengono memorizzati nel repository.
  - *x* **di** *y* **Scaricato**. Non tutti gli aggiornamenti firmware nel pacchetto di aggiornamento sono memorizzati nel repository. I numeri tra parentesi indicano il numero di aggiornamenti disponibili e il

numero di aggiornamenti memorizzati, oppure l'indisponibilità di aggiornamenti per il tipo di dispositivo specifico.

– **Non scaricato**. L'intero pacchetto di aggiornamento o i singoli aggiornamenti firmware sono disponibili ma non sono memorizzati nel repository.

Quando si installa XClarity Administrator o si esegue l'aggiornamento a una nuova release, è consigliabile scaricare il pacchetto del repository più recente per essere certi di disporre degli ultimi aggiornamenti firmware. Quindi, è possibile pianificare un processo ricorrente per aggiornare il catalogo e individuare i singoli aggiornamenti pubblicati sul Web dall'ultimo pacchetto del repository, per poi scaricare elettronicamente gli aggiornamenti, uno alla volta.

XClarity Administrator deve essere collegato a Internet per aggiornare il catalogo e scaricare gli aggiornamenti firmware. Se non è collegato a Internet, è possibile scaricare manualmente i file in una workstation che ha accesso alla rete nell'host XClarity Administrator, tramite un browser Web e quindi importare i file nel repository degli aggiornamenti firmware.



Quando si importano manualmente gli aggiornamenti firmware in XClarity Administrator, è necessario includere i seguenti file: payload (immagine e MIB), metadati, cronologia delle modifiche e readme. Ad esempio:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Nota: Gli aggiornamenti firmware principali (come il controller di gestione, UEFI e pDSA) sono indipendenti del sistema operativo. I pacchetti di aggiornamento firmware per i sistemi operativi RHEL 6 o SLES 11 sono utilizzati per aggiornare i nodi di elaborazione e i server rack.

Un messaggio viene visualizzato sulla pagina quando il repository è pieno almeno al 50%. Un altro messaggio viene visualizzato sulla pagina quando il repository è pieno almeno all'85%. Per ridurre lo spazio utilizzato nel repository, è possibile rimuovere i criteri e i file di immagine inutilizzati. È possibile rimuovere i criteri di conformità del firmware non utilizzati e i pacchetti del firmware ad essi associati facendo clic su **Provisioning → Criteri di conformità**, selezionando uno o più criteri da eliminare e facendo quindi clic su **Azioni → Elimina qualsiasi pacchetto firmware e criterio**.

La seguente tabella riepiloga le differenze tra l'acquisizione dei pacchetti del repository degli aggiornamenti firmware, dei pacchetti UXSPs e dei singoli pacchetti di aggiornamento firmware.

Pacchetto di aggiornamento	Pagina di interfaccia utente per il download e l'importazione dei file	Pagina Web per il download manuale dei file	Il repository degli aggiornamenti firmware è stato aggiornato?	I criteri di conformità del firmware sono stati aggiornati automaticamente?
Pacchetti del repository degli aggiornamenti firmware	Pagina Aggiorna server di gestione **Nota:** È necessario importare e successivamente applicare il pacchetto del repository.	Pagina Web di download di XClarity Administrator	Sì	Sì
UpdateXpress System Packs	Pagina Aggiornamenti firmware: Repository, scheda **UpdateXpress System Packs (UXSPs)**	Pagina Web di Lenovo XClarity Essentials UpdateXpress	Sì	Sì
Aggiornamenti firmware	Pagina Aggiornamenti firmware: Repository, scheda **Aggiornamenti individuali**	Sito Web dell'Assistenza del Centro Dati Lenovo **Nota:** Utilizzare sito Web di Fix Central per i seguenti dispositivi: • Flex System x220 Tipo 2585, 7906 • Nodo di elaborazione Flex System x222 Tipo 2589, 7916 • Flex System x240 Tipo 7863, 8737, 8738, 8956 • Flex System x280/x480/ x880 X6 Tipo 4259, 7903 • Flex System x440 Tipo 2584, 7917	Sì	No

Procedura

Per scaricare uno o più aggiornamenti firmware, completare le seguenti operazioni:

- Per importare uno o più *pacchetti del repository degli aggiornamenti firmware*:
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Aggiorna server di gestione** per visualizzare la pagina Aggiornamento server di gestione.
  2. Scaricare i pacchetti del repository più recenti:
     - Se XClarity Administrator è collegato a Internet:
       a. Recuperare le informazioni sugli aggiornamenti più recenti facendo clic sull'icona **Aggiorna catalogo → Aggiorna tutti gli elementi gestiti - Solo i più recenti**. I nuovi aggiornamenti del server di gestione e i nuovi pacchetti del repository degli aggiornamenti firmware sono elencati nella tabella nella pagina "Aggiornamento server di gestione".

          Il completamento dell'aggiornamento del repository potrebbe richiedere diversi minuti.

Nota: L'aggiornamento del repository non include il download automatico dei file payload. Solo i file dei metadati e readme vengono scaricati.

b. Selezionare i pacchetti del repository degli aggiornamenti firmware che si desidera scaricare.

Suggerimento: accertarsi che i pacchetti selezionati siano contrassegnati dal valore "Pacchetto supplementare" nella colonna **Tipo**.

c. Fare clic sull'icona **Scarica elementi selezionati** (). Al termine del download, il valore **Stato download** per tale aggiornamento software viene modificato in "Scaricato".

– Se XClarity Administrator non è collegato a Internet:

a. Scaricare i pacchetti del repository degli aggiornamenti firmware da Pagina Web di download di XClarity Administrator in una workstation con connessione di rete nell'host XClarity Administrator.

b. Nella pagina Aggiornamento server di gestione, fare clic sull'icona **Importa** ().

c. Fare clic su **Seleziona file** e selezionare la posizione dei pacchetti del repository degli aggiornamenti firmware sulla workstation.

d. Selezionare tutti i file di pacchetto, quindi fare clic su **Apri**.

È necessario importare il file di metadati (.xml o .json) nonché i file di immagine e del payload (.zip, .bin, .uxz o .tgz), il file della cronologia delle modifiche (.chg) e il file readme (.txt) per l'aggiornamento. Tutti i file selezionati ma non specificati nel file dei metadati vengono eliminati. Se non si include il file dei metadati, l'aggiornamento non viene importato.

e. Fare clic su **Importa**.

Una volta completata l'importazione, i pacchetti del repository degli aggiornamenti firmware sono elencati nella tabella della pagina Aggiornamento server di gestione e il valore di **Stato download** di ciascun aggiornamento è "Scaricato".

3. Selezionare i pacchetti del repository degli aggiornamenti firmware che si desidera installare nel repository degli aggiornamenti firmware.

Nota: Accertarsi che il valore di **Stato download** sia "Scaricato" e che **Tipo** sia impostato su "Patch."

4. Fare clic sull'icona **Esegui aggiornamento** () per aggiungere i pacchetti di aggiornamento firmware al repository.
5. Attendere alcuni minuti per consentire il completamento dell'aggiornamento e il riavvio di XClarity Administrator.
6. Determinare se l'aggiornamento è completo aggiornando il browser Web.

Al termine dell'operazione, viene visualizzata la pagina Aggiornamento server di gestione e il valore della colonna **Stato applicato** viene modificato in "Applicato".

7. Cancellare la cache del browser Web.

- Per scaricare uno o più pacchetti *UXSP*.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Repository** per visualizzare la pagina Repository aggiornamenti firmware.
2. Fare clic sulla scheda **UpdateXpress System Packs (UXSPs)**.
3. Scaricare i pacchetti UXSP più recenti:

– Se XClarity Administrator è collegato a Internet:

Per aggiornare il catalogo e scaricare i pacchetti UXSP più recenti per tutti i dispositivi gestiti, fare clic su **Tutte le azioni → Aggiorna e scarica la versione più recente per tutti i dispositivi gestiti**.

Per aggiornare il catalogo e scaricare i pacchetti UXSP più recenti solo per i dispositivi selezionati:

a. Espandere la vista del dispositivo per visualizzare l'elenco dei pacchetti UXSP disponibili.
b. Selezionare uno o più pacchetti UXSP che si desidera scaricare.
c. Fare clic su **Tutte le azioni → Aggiorna e scarica la versione più recente per i dispositivi selezionati**.

   Al termine del download, il valore **Stato download** per i pacchetti UXSP selezionati viene modificato in "Scaricato".

– Se XClarity Administrator non è collegato a Internet:

a. Scaricare i pacchetti UXSP dal Pagina Web di Lenovo XClarity Essentials UpdateXpress in una workstation con connessione di rete all'host XClarity Administrator.
b. Da XClarity Administrator, fare clic sull'icona **Importa** ().
c. Fare clic su **Seleziona file** e selezionare la posizione del pacchetto UXSP sulla workstation.
d. Selezionare tutti i file di pacchetto, quindi fare clic su **Apri**.

   È necessario importare il file di metadati (.xml o .json) nonché i file di immagine e del payload (. zip, .bin, .uxz o .tgz), il file della cronologia delle modifiche (.chg) e il file readme (.txt) per l'aggiornamento. Tutti i file selezionati ma non specificati nel file dei metadati vengono eliminati. Se non si include il file dei metadati, l'aggiornamento non viene importato.
e. Fare clic su **Importa**.

   Una volta completata l'importazione, i pacchetti del repository degli aggiornamenti firmware sono elencati nella tabella della pagina Aggiornamento server di gestione e il valore di Stato download di ciascun aggiornamento è "Scaricato."

- Per scaricare uno o più *pacchetti di aggiornamento firmware* individuali.
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Repository** per visualizzare la pagina Repository aggiornamenti firmware.
  2. Se si sta scaricando il firmware per i dispositivi di storage ThinkSystem della serie DM, selezionare il paese in si trovano cui tali dispositivi.
  3. Fare clic sulla scheda **Aggiornamenti individuali**.
  4. Scaricare i più recenti aggiornamenti firmware individuali:

     – Se XClarity Administrator è collegato a Internet:

     Per aggiornare il catalogo e scaricare il firmware più recente per tutti i dispositivi gestiti, fare clic su **Tutte le azioni → Aggiorna e scarica la versione più recente per tutti i dispositivi gestiti**.

     Per aggiornare il catalogo e scaricare il firmware più recente solo per i dispositivi selezionati:

     a. Espandere la vista del dispositivo per visualizzare l'elenco degli aggiornamenti firmware disponibili.
     b. Selezionare uno o più aggiornamenti firmware che si desidera scaricare.

        Suggerimento: un pacchetto di aggiornamento può essere composto da più aggiornamenti firmware. Quando si scarica un aggiornamento firmware, è possibile scegliere di scaricare l'intero pacchetto di aggiornamento o solo aggiornamenti specifici. È anche possibile scegliere di scaricare più pacchetti contemporaneamente.
     c. Fare clic su **Tutte le azioni → Aggiorna e scarica la versione più recente per i dispositivi selezionati**.

        Al termine del download, il valore **Stato download** per gli aggiornamenti firmware selezionati viene modificato in "Scaricato".

- Se XClarity Administrator non è collegato a Internet:
  a. Scaricare i pacchetti di aggiornamento firmware da Sito Web dell'Assistenza del Centro Dati Lenovo in una workstation con connessione di rete nell'host XClarity Administrator.

     Per i seguenti server, scaricare gli aggiornamenti firmware per il sistema operativo SLES 11 da sito Web di Fix Central:

     - Flex System x220 Tipo 2585, 7906
     - Nodo di elaborazione Flex System x222 Tipo 2589, 7916
     - Flex System x240 Tipo 7863, 8737, 8738, 8956
     - Flex System x280/x480/x880 X6 Tipo 4259, 7903
     - Flex System x440 Tipo 2584, 7917

     Per tutti gli altri server, scaricare gli aggiornamenti firmware per il sistema operativo RHEL 6 da Sito Web del supporto per Lenovo XClarity:

  b. Da XClarity Administrator, fare clic sull'icona **Importa** ().
  c. Fare clic su **Seleziona file** e selezionare la posizione degli aggiornamenti firmware sulla workstation.
  d. Selezionare tutti i file di pacchetto, quindi fare clic su **Apri**.

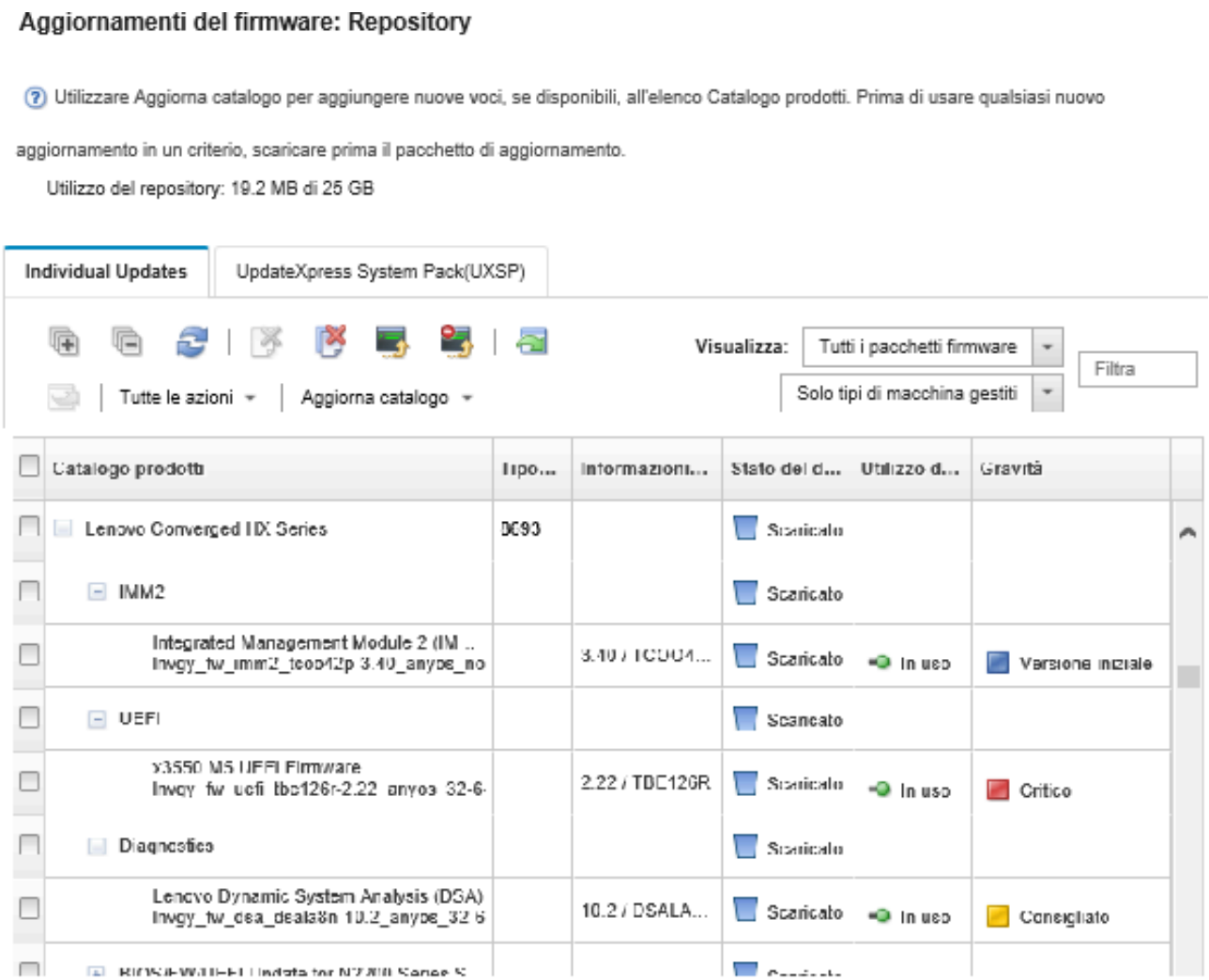
     È necessario importare il file di metadati (.xml o .json) nonché i file di immagine e del payload (. zip, .bin, .uxz o .tgz), il file della cronologia delle modifiche (.chg) e il file readme (.txt) per l'aggiornamento. Tutti i file selezionati ma non specificati nel file dei metadati vengono eliminati.

     Attenzione:

     - Importare solo questi file obbligatori. Non importare altri file che potrebbero essere disponibili nei siti Web di download del firmware.
     - Se non si include il file XML nel pacchetto di aggiornamento, l'aggiornamento non viene importato.
     - Se non si includono tutti i file richiesti associati all'aggiornamento, il repository contrassegna l'aggiornamento come non scaricato, ad indicare che è stato parzialmente importato. È quindi possibile importare i file mancanti selezionandoli e importandoli.
     - Gli aggiornamenti firmware principali (come il controller di gestione, UEFI e pDSA) sono indipendenti del sistema operativo. I pacchetti di aggiornamento firmware per i sistemi operativi RHEL 6 o SLES 11 sono utilizzati per aggiornare i nodi di elaborazione e i server rack. Per ulteriori informazioni sui pacchetti di aggiornamento firmware da utilizzare per i server gestiti, vedere Download degli aggiornamenti firmware.
  e. Fare clic su **Importa**.

L'aggiornamento del catalogo e il download degli aggiornamenti firmware potrebbero richiedere alcuni minuti. Quando gli aggiornamenti sono stati scaricati e memorizzati nel repository, la riga nel catalogo prodotti viene evidenziata e il valore della colonna **Stato download** viene modificato in "Scaricato".

Nota: Il tipo di macchina per alcuni switch potrebbe essere visualizzato come numero esadecimale.



Al termine

È possibile configurare la dimensione massima del repository degli aggiornamenti (inclusi firmware, driver di dispositivo del sistema operativo e aggiornamenti del server di gestione) dalla pagina Repository del firmware, facendo clic su **Tutte le azioni → Impostazioni globali**. La dimensione minima è di 50 GB. La dimensione massima dipende dalla quantità di spazio sul disco del sistema locale.

Esportazione e importazione degli aggiornamenti firmware

È possibile esportare nel sistema locale i singoli aggiornamenti firmware e i UpdateXpress System Packs (UXSPs) disponibili nel repository.

Informazioni su questa attività

Vengono esportati solo gli aggiornamenti presenti nel repository. Verificare che lo stato del download degli aggiornamenti firmware selezionati sia "Scaricato."

Vengono esportati tutti i file associati all'aggiornamento firmware, inclusi l'immagine di aggiornamento o il file payload (.zip, .bin, .uxz o .tgz), il file dei metadati (.xml o .json), il file della cronologia delle modifiche (.chg) e il file readme (.txt).

Attenzione: Non modificare il nome dei file di aggiornamento firmware.

Procedura

- Per esportare gli aggiornamenti firmware:
  1. Fare clic sulla scheda **Aggiornamenti individuali** o sulla scheda **UpdateXpress System Packs (UXSPs)**.
  2. Selezionare uno o più aggiornamenti firmware.
  3. Fare clic sull'icona **Esporta** ().
- Per importare gli aggiornamenti firmware:

  È possibile importare manualmente i file esportati da Lenovo XClarity Administrator e i file scaricati manualmente dal Web. Per ulteriori informazioni, vedere Download degli aggiornamenti firmware.

Eliminazione degli aggiornamenti firmware

È possibile eliminare gli aggiornamenti firmware e i pacchetti UpdateXpress System Packs (UXSPs) dal repository degli aggiornamenti firmware.

Prima di iniziare

Accertarsi che tutti i processi di aggiornamento in esecuzione o pianificati che utilizzano criteri di conformità del firmware e contengono aggiornamenti firmware da eliminare vengano completati o annullati (vedere Monitoraggio dei processi).

Accertarsi che l'aggiornamento non sia in uso nei criteri di conformità del firmware prima di procedere all'eliminazione. Non è possibile eliminare i pacchetti di aggiornamento firmware attualmente utilizzati in uno o più criteri di conformità del firmware.

L'eliminazione di un pacchetto UXSP comporta anche l'eliminazione dei criteri di conformità del firmware creati automaticamente per tale pacchetto UXSP.

Nota: Prestare attenzione quando si eliminano gli aggiornamenti firmware e gli UXSP se il repository degli aggiornamenti firmware è una condivisione remota utilizzata da più istanze di XClarity Administrator.

Procedura

Per eliminare uno o più aggiornamenti firmware dal repository, completare le seguenti operazioni.

Passo 1. Annullare l'assegnazione dei criteri di conformità del firmware che contengono gli aggiornamenti firmware da eliminare da tutti i dispositivi gestiti.

   a. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Applica/Attiva**. Viene visualizzata la pagina Aggiornamenti firmware: Applica/Attiva.

   b. Scegliere "Nessuna assegnazione" oppure selezionare altri criteri di conformità del firmware nella colonna **Criteri assegnati** per i dispositivi gestiti che utilizzano i criteri di conformità del firmware.

Passo 2. Eliminare tutti i criteri di conformità del firmware definiti dall'utente che contengono gli aggiornamenti firmware da eliminare o i criteri di conformità del firmware modificati per rimuovere gli aggiornamenti firmware da eliminare.

   a. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Criteri di conformità**. Viene visualizzata la pagina Criteri di conformità aggiornamenti firmware.

b. Selezionare i criteri di conformità del firmware e quindi l'icona **Elimina** () per eliminare i criteri oppure fare clic sull'icona **Modifica** () per rimuovere gli aggiornamenti firmware dai criteri.

Passo 3. Eliminare gli aggiornamenti firmware.

- **Aggiornamenti firmware individuali**
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Repository**. Viene visualizzata la pagina Repository aggiornamenti firmware.
  2. Fare clic sulla scheda **Aggiornamenti individuali**.
  3. Selezionare uno o più aggiornamenti firmware da eliminare.
  4. Fare clic sull'icona **Elimina solo le immagini** () per eliminare solo l'immagine o il file payload (.zip, .bin, .uxz o .tgz). Le informazioni sull'aggiornamento non vengono rimosse, in modo da semplificare un eventuale nuovo download dell'aggiornamento. Oppure fare clic sull'icona **Elimina pacchetti di aggiornamento completi** () per eliminare i pacchetti di aggiornamento completi, inclusi l'immagine o il file payload, il file di cronologia delle modifiche (.chg), il file readme (.txt) e il file dei metadati (.xml o .json).

  Quando si elimina un aggiornamento firmware, i file di payload vengono rimossi; il file dei metadati, che contiene informazioni sull'aggiornamento, non viene invece rimosso, in modo da semplificare un eventuale nuovo download dell'aggiornamento, se necessario, mentre la voce **Stato del download** viene modificata in "Non scaricato".
- **UXSP**
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Repository**. Viene visualizzata la pagina Repository aggiornamenti firmware.
  2. Fare clic sulla scheda **UpdateXpress System Pack (UXSP)**.
  3. Selezionare uno o più pacchetti UXSP da eliminare.
  4. Fare clic sull'icona **Elimina UXSP e criterio associato** () per eliminare i pacchetti UXSP completi, inclusi l'immagine o il file payload, il file di cronologia delle modifiche (.chg), il file readme (.txt), il file dei metadati (.xml o .json) e tutti i criteri di conformità associati del firmware.

  Se i pacchetti UXSP selezionati sono associati a criteri utilizzati (assegnati ai dispositivi), viene visualizzata la finestra di dialogo Elimina UXSP, criteri e pacchetti di aggiornamento. Scegliere se eliminare i criteri assegnati, oltre ai pacchetti UXSP e ai criteri non assegnati e fare clic su **OK**.

Creazione e assegnazione di criteri di conformità del firmware

criteri di conformità del firmware permettono di verificare che il livello di firmware di determinati dispositivi gestiti sia al livello corrente o specificato, contrassegnando i dispositivi che richiedono attenzione. Ogni criterio di conformità del firmware identifica i dispositivi monitorati e il livello firmware da installare per mantenere la conformità dei dispositivi. È possibile impostare la conformità a livello di dispositivo o componente firmware. XClarity Administrator utilizza quindi questi criteri per controllare lo stato dei dispositivi gestiti e identificare i dispositivi non conformi.

Prima di iniziare

Quando si crea un criterio di conformità del firmware, è necessario selezionare la versione dell'aggiornamento di destinazione da applicare ai dispositivi che verranno assegnati al criterio. Verificare che gli aggiornamenti del firmware per la versione di destinazione si trovino nel repository degli aggiornamenti prima di creare i criteri (vedere Download degli aggiornamenti firmware).

Se un tipo di dispositivo non è elencato nel repository degli aggiornamenti firmware, è necessario gestire un dispositivo di quel tipo e quindi scaricare o importare la serie completa degli aggiornamenti firmware prima di creare i criteri di conformità per dispositivi di tale tipo.

Informazioni su questa attività

Quando si creano dei criteri di conformità del firmware, è possibile configurare XClarity Administrator in modo che contrassegni un dispositivo nei seguenti casi:
- Il firmware del dispositivo è di livello inferiore a quello richiesto
- Il firmware del dispositivo non corrisponde esattamente alla versione dell'obiettivo di conformità

XClarity Administrator è dotato di criteri di conformità del firmware predefiniti denominati **Firmware più recente nel repository**. Quando il nuovo firmware viene scaricato o importato nel repository, questo criterio viene aggiornato per includere le versioni di firmware più recenti nel repository.

Una volta assegnati a un dispositivo i criteri di conformità del firmware, XClarity Administrator verifica lo stato di conformità di ogni dispositivo ogni volta che vengono apportate modifiche all'inventario del dispositivo o a un repository degli aggiornamenti firmware. Quando il firmware di un dispositivo non è conforme ai criteri assegnati, XClarity Administrator identifica il dispositivo come non conforme nella pagina Aggiornamenti firmware: Applica/Attiva, in base alla regola specificata nei criteri di conformità del firmware.

Ad esempio, è possibile creare criteri di conformità del firmware che definiscono il livello di riferimento per il firmware installato in tutti i dispositivi ThinkSystem SR850 e quindi assegnare i criteri di conformità del firmware a tutti i dispositivi ThinkSystem SR850 gestiti. Quando il repository degli aggiornamenti firmware viene aggiornato e viene aggiunto un nuovo aggiornamento firmware, tali nodi di elaborazione potrebbero diventare non conformi. Quando ciò si verifica, XClarity Administrator aggiorna la pagina Aggiornamenti firmware: Applica/Attiva per contrassegnare tali dispositivi come non conformi e genera un avviso.

Nota: È possibile scegliere di visualizzare o nascondere gli avvisi per i dispositivi che non soddisfano i requisiti dei criteri di conformità del firmware assegnati (vedere Configurazione delle impostazioni globali di aggiornamento del firmware). Gli avvisi vengono nascosti per impostazione predefinita.

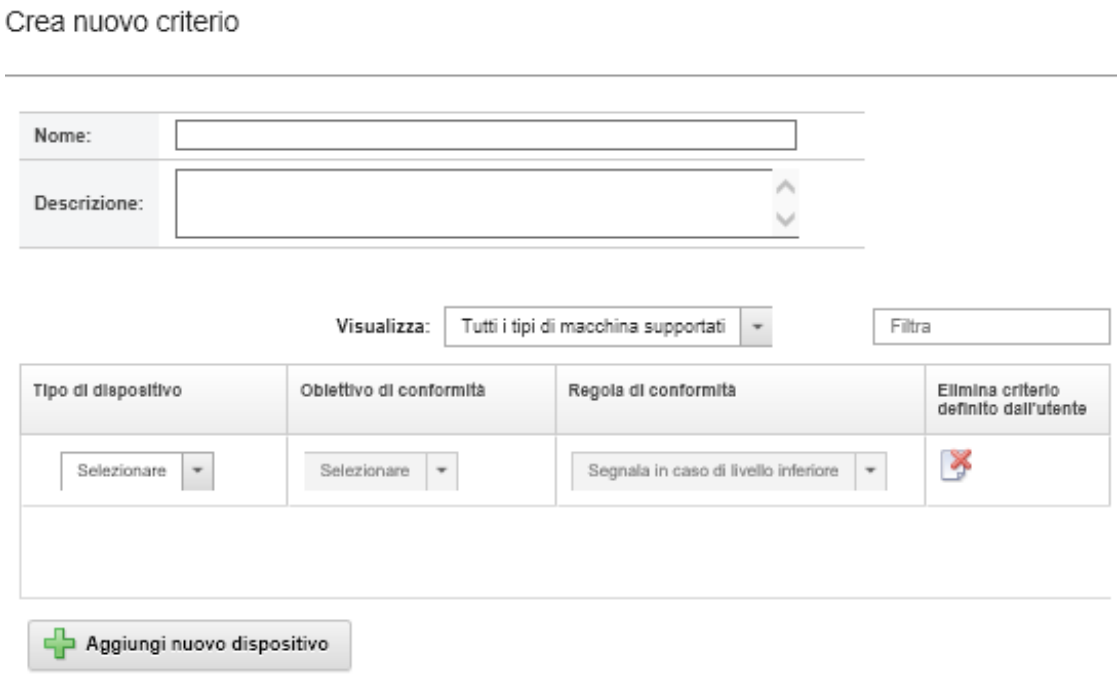
Procedura

Per creare e assegnare un criterio di conformità del firmware, completare la procedura che segue.

Passo 1. Sulla barra dei menu di XClarity Administrator fare clic su **Provisioning → Aggiornamenti firmware: Criteri di conformità**. Viene visualizzata la pagina Criteri di conformità contenente un elenco di tutti i criteri di conformità del firmware esistenti.

Passo 2. Creare un criterio di conformità del firmware.

1. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo Crea nuovi criteri.



2. Compilare il nome e la descrizione del criterio di conformità del firmware.
3. Compilare la tabella in base ai criteri che seguono per ciascun dispositivo.
   - **Tipo di dispositivo**. Scegliere un tipo di dispositivo o componente per cui applicare questo criterio.

     Suggerimento: se si sceglie un server, il livello di conformità viene stabilito a livello di UXSP. Tuttavia, è anche possibile espandere il server per specificare i livelli specifici di firmware per ciascun componente, quali il controller di gestione della baseboard o UEFI.
   - **Obiettivo di conformità**. Specificare l'obiettivo di conformità per i dispositivi e i componenti secondari applicabili.

     Per i server, è possibile scegliere uno dei seguenti valori.

     – **Predefinito**. Modifica l'obiettivo di conformità per ciascun componente secondario impostando il valore predefinito (ad esempio, la serie più recente del firmware nel repository per il dispositivo).

– **Non aggiornare**. Modifica l'obiettivo di conformità per ciascun componente secondario in "Non aggiornare."

Per i dispositivi senza componenti secondari (come CMM, switch o dispositivi di storage) o per i componenti secondari di un server, è possibile scegliere uno dei seguenti valori.

– <*firmware_level*>. Specifica il livello di firmware di base.

– **Non aggiornare**. Specifica che il firmware non deve essere aggiornato. Tenere presente che il firmware del controller di gestione di backup non viene aggiornato per impostazione predefinita.

Nota: Quando si modificano i valori predefiniti per qualsiasi componente secondario di un server, l'obiettivo di conformità per il server viene modificato in **Personalizzato**.

- **Regola di conformità**. Specificare quando un dispositivo è contrassegnato come non conforme nella colonna **Versione installata** di Aggiornamenti firmware: Applica/Attiva.

  – **Segnala in caso di livello inferiore**. Se il livello di firmware installato su un dispositivo è inferiore rispetto a quanto specificato nei criteri di conformità del firmware, il dispositivo è contrassegnato come non conforme. Se, ad esempio, si sostituisce una scheda di rete in un nodo di elaborazione e il firmware della scheda di rete è di un livello precedente rispetto a quanto identificato nei criteri di conformità del firmware, il nodo di elaborazione viene contrassegnato come non conforme.

  – **Segnala in caso di coincidenza non esatta**. Se il livello di firmware installato su un dispositivo non corrisponde esattamente ai criteri di conformità del firmware, il dispositivo è contrassegnato come non conforme. Se, ad esempio, si sostituisce una scheda di rete in un nodo di elaborazione e il firmware della scheda di rete è di un livello diverso rispetto a quanto identificato nei criteri di conformità del firmware, il nodo di elaborazione viene contrassegnato come non conforme.

  – **Nessuna segnalazione**. I dispositivi non conformi non vengono segnalati.

4. **Facoltativo:** espandere il tipo di sistema per visualizzare ciascun aggiornamento nel pacchetto e selezionare il livello di firmware da utilizzare come obiettivo di conformità; in alternativa, selezionare "Non aggiornare" per impedire l'aggiornamento del firmware su quel dispositivo.
5. Fare clic su **Crea**.

   I criteri di conformità del firmware sono elencati nella tabella della pagina Aggiornamenti firmware: Criterio di conformità. La tabella riporta lo stato di utilizzo, l'origine dei criteri (se definiti dall'utente o predefiniti) e l'ultima data di modifica.

Passo 3. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Applica/Attiva**. Viene visualizzata la pagina Aggiornamenti firmware: Applica/Attiva con l'elenco dei dispositivi gestiti.

Passo 4. Assegnare i criteri di conformità del firmware ai dispositivi.

- **Per un singolo dispositivo**

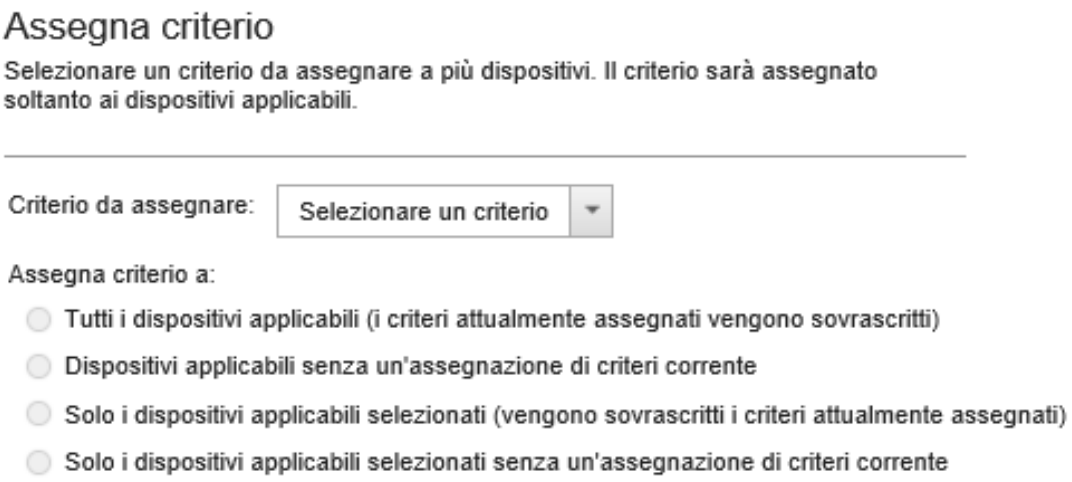
  Per ciascun dispositivo selezionare un criterio dal menu a discesa nella colonna **Criterio di conformità assegnato**.

  È possibile scegliere da un elenco dei criteri di conformità del firmware applicabili a ciascun dispositivo. Se un criterio non è attualmente assegnato al dispositivo, il criterio assegnato è impostato su **Nessuna assegnazione**. Se non vi sono criteri applicabili al dispositivo, il criterio assegnato è impostato su **Nessun criterio applicabile**.

- **Per più dispositivi**

  1. **Facoltativo:** selezionare uno o più dispositivi a cui assegnare criteri di conformità del firmware.

2. Fare clic sull'icona **Assegna criterio** ( ) per visualizzare la relativa finestra di dialogo.



3. Selezionare i criteri di conformità dal menu a discesa **Criteri da assegnare**.

   È possibile scegliere da un elenco dei criteri di conformità del firmware applicabili a tutti i dispositivi selezionati. Se i dispositivi non sono stati selezionati prima di aprire la finestra di dialogo, vengono elencati tutti i criteri.

   Per annullare l'assegnazione di un criterio, selezionare **Nessuna assegnazione**.

4. Selezionare uno dei seguenti ambiti per l'assegnazione dei criteri.
   - **Tutti i dispositivi applicabili che sono...**
   - **Solo i dispositivi applicabili selezionati che sono…**
5. Selezionare uno o più criteri del dispositivo.
   - **Senza un criterio assegnato**
   - **Non conformi (sovrascrivere i criteri attualmente assegnati)**
   - **Conformi (sovrascrivere i criteri attualmente assegnati)**
   - **Non monitorati (sovrascrivere i criteri attualmente assegnati)**
   - **Altri (sovrascrivere i criteri attualmente assegnati)**. Questa operazione si applica ai dispositivi che si trovano in altri stati, ad esempio nello stato In sospeso, con dati mancanti o non supportati per gli aggiornamenti. Passare il mouse sull'icona Guida ( ) per visualizzare un elenco di dispositivi applicabili.

   Nota: I criteri **Non monitorati** e **Altri** sono elencati solo quando sono presenti dispositivi in tali stati.
6. Fare clic su **OK**.

   Il nome dei criteri assegnati nella colonna **Criteri assegnati** della pagina "Aggiornamenti firmware: repository" viene modificato in base al nome dei criteri di conformità del firmware selezionati.

Al termine

Dopo aver creato i criteri di conformità del firmware, eseguire le azioni indicate di seguito sui singoli criteri di conformità del firmware selezionati:

- Visualizzare i dettagli dei criteri, incluso un elenco di dispositivi assegnati, facendo clic sul nome dei criteri nella tabella.

- Creare un duplicato di un criterio selezionato facendo clic sull'icona **Copia** ( ).
- Rinominare o modificare un criterio selezionato facendo clic sull'icona **Modifica** ( ).Non è possibile modificare un criterio di conformità del firmware predefinito o un criterio assegnato a un dispositivo gestito.

  Se si modifica un criterio assegnato in modo tale da non applicarlo più a determinati dispositivi assegnati, l'assegnazione di tale criterio viene automaticamente annullata per tali dispositivi.

  Non è possibile rinominare o modificare il criterio **Firmware più recente**.
- Eliminare un criterio di conformità del firmware selezionato facendo clic sull'icona **Elimina criterio** ( ) oppure eliminare il criterio di conformità del firmware selezionato e tutti gli aggiornamenti firmware associati utilizzati soltanto da tale criterio facendo clic sull'icona **Elimina qualsiasi pacchetto firmware e criterio** ( ).È possibile scegliere di eliminare il criterio anche se è assegnato a un dispositivo.

  Quando si elimina un criterio assegnato a un dispositivo, prima di eliminarlo viene annullata l'assegnazione.

  Non è possibile eliminare i criteri **Firmware più recente** predefiniti, ma è possibile disabilitarli facendo clic sull'icona **Impostazioni globali** ( ) e quindi selezionando **Disabilita criteri firmware più recenti**. Quando questa opzione è selezionata, il criterio firmware più recente non viene assegnato ai dispositivi gestiti e non viene più aggiornato per includere le versioni del firmware più recenti disponibili nel repository.
- Esportare un criterio selezionato in un sistema locale selezionando i criteri e facendo clic sull'icona **Esporta** ( ). È quindi possibile importare i criteri in un'altra istanza di XClarity Administrator facendo clic sull'icona **Importa** ( ).

Una volta creati, i criteri di conformità del firmware possono essere assegnati a un dispositivo specifico (vedere Creazione e assegnazione di criteri di conformità del firmware) ed è inoltre possibile applicare e attivare gli aggiornamenti per tale dispositivo (vedere Applicazione e attivazione degli aggiornamenti firmware).

Identificazione dei dispositivi non conformi

Se sono stati assegnati criteri di conformità del firmware a un dispositivo gestito, è possibile determinare se il firmware di tale dispositivo è conforme a tali criteri.

Procedura

Per determinare se il firmware su un dispositivo è conforme ai criteri di conformità del firmware assegnati, fare clic su **Provisioning → Aggiornamenti firmware: Applica/Attiva** nella barra del menu di Lenovo XClarity Administrator per visualizzare la pagina Aggiornamento firmware: criteri di conformità e verificare la colonna **Versioni installate** per tale dispositivo.

La colonna **Versioni installate** contiene uno dei seguenti valori:

- **Versione firmware**. La versione firmware installata sul dispositivo è conforme ai criteri assegnati.
- **Conforme**. Il firmware installato sul dispositivo è conforme ai criteri assegnati.
- **Non conforme**. Il firmware installato sul dispositivo non è conforme ai criteri assegnati.
- **Nessun criterio di conformità impostato**. Nessun criterio di conformità del firmware è assegnato al dispositivo.

È possibile fare clic sull'icona **Aggiorna** ( ) per aggiornare il contenuto nella colonna **Versione installata**.

Configurazione delle impostazioni globali di aggiornamento del firmware

Le impostazioni globali fungono da impostazioni predefinite quando vengono applicati gli aggiornamenti firmware.

Informazioni su questa attività

Nella pagina Impostazioni globali è possibile configurare le seguenti impostazioni:
- Supporto potenziato per dispositivi di livello inferiore
- Avvisi per i dispositivi non conformi ai criteri assegnati
- Assegnazione automatica dei criteri di conformità del firmware per un dispositivo senza criteri assegnati
- Stato di non conformità per i dispositivi con un componente firmware privo di destinazione associata nei criteri di conformità del firmware

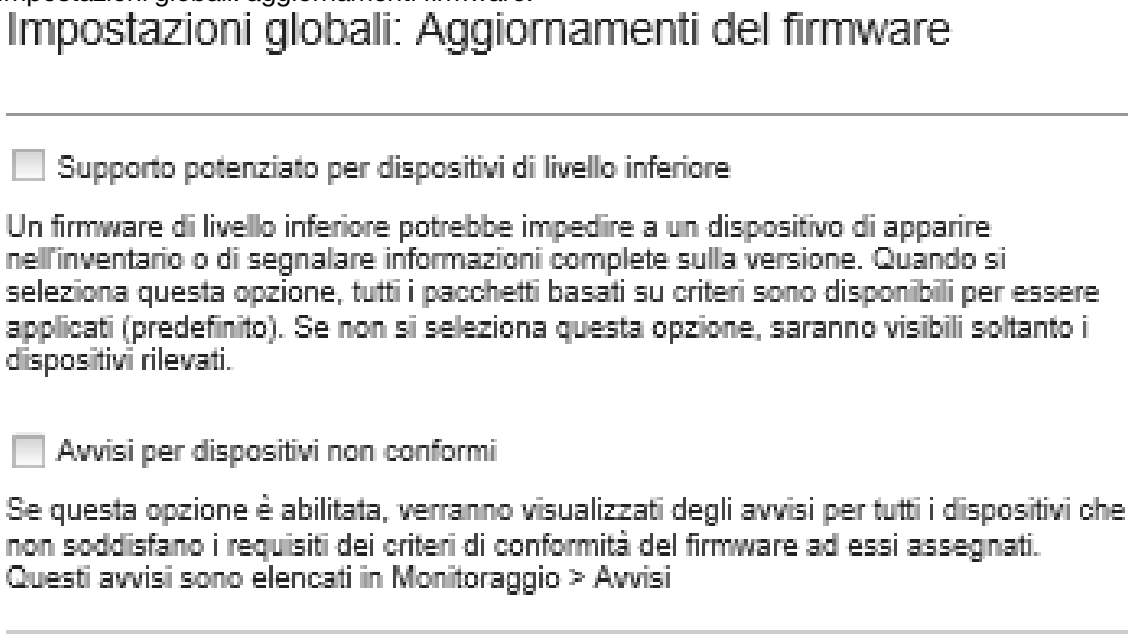
Procedura

Per configurare le impostazioni globali da utilizzare per tutti i server, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Applica/Attiva**. Viene visualizzata la pagina Aggiornamenti firmware: Applica/Attiva.

Passo 2. Fare clic sulla scheda **Aggiorna con criterio** o **Aggiorna senza criterio**.

Passo 3. Fare clic su **Tutte le azioni → Impostazioni globali** per visualizzare la finestra di dialogo Impostazioni globali: aggiornamenti firmware.



Passo 4. Facoltativamente, selezionare una delle seguenti opzioni:

- Selezionare **Supporto potenziato per dispositivi di livello inferiore** per visualizzare le informazioni su inventario e versione completa per tutti i dispositivi, anche se il firmware è di livello inferiore o se il dispositivo non è presente nell'inventario.
- Selezionare **Avvisi per i dispositivi non conformi** per visualizzare gli avvisi nella pagina degli avvisi per i dispositivi che non soddisfano i requisiti dei criteri di conformità del firmware assegnati. Per impostazione predefinita, gli avvisi vengono nascosti nella pagina degli avvisi. Per ulteriori informazioni, vedere Visualizzazione di avvisi attivi.
- Selezionare **Disabilita assegnazione criteri automatici** per disabilitare l'assegnazione automatica dei criteri di conformità del firmware per un dispositivo senza criteri assegnati. Se

questa opzione non è selezionata, i criteri di conformità del firmware vengono assegnati ai dispositivi senza criteri, una volta riavviato XClarity Administrator o quando si gestisce un nuovo dispositivo.

- Selezionare **Report non conforme per il firmware senza destinazione** per contrassegnare i dispositivi come non conformi, quando un componente del firmware non dispone di una destinazione associata nei criteri di conformità del firmware. Se questa opzione non è selezionata, i dispositivi senza destinazioni vengono contrassegnati come conformi.

Passo 5. Fare clic su **OK** per chiudere la finestra di dialogo.

Applicazione e attivazione degli aggiornamenti firmware

Lenovo XClarity Administrator non applica automaticamente gli aggiornamenti firmware ai dispositivi gestiti. È possibile scegliere di applicare gli aggiornamenti firmware con o senza i criteri di conformità.

Prima di iniziare

Quando si utilizzano i criteri di conformità, è possibile pianificare gli aggiornamenti su più dispositivi contemporaneamente. XClarity Administrator aggiorna automaticamente i dispositivi nella sequenza corretta. Il CMM viene aggiornato per primo, seguito dagli switch, dai server e quindi dai dispositivi di storage.

Solo gli aggiornamenti firmware scaricati possono essere applicati.

Quando si esegue un aggiornamento firmware, XClarity Administrator avvia uno o più processi per eseguire l'aggiornamento.

Mentre l'aggiornamento firmware è in corso, il dispositivo di destinazione è bloccato. Non è possibile avviare altre attività di gestione sul dispositivo di destinazione finché il processo di aggiornamento non è completo.

Una volta applicato un aggiornamento firmware a un dispositivo, potrebbero essere necessari uno o più riavvii per attivare completamente l'aggiornamento firmware. È possibile scegliere se riavviare il dispositivo immediatamente, ritardare l'attivazione o dare priorità all'attivazione. Se si sceglie il riavvio immediato, XClarity Administrator riduce al minimo il numero di riavvii richiesti. Se si sceglie l'attivazione ritardata, gli aggiornamenti vengono attivati al successivo riavvio del dispositivo. Se si sceglie di dare priorità all'attivazione, gli aggiornamenti vengono attivati immediatamente sul controller di gestione della scheda di base e tutti gli altri aggiornamenti firmware vengono attivati al successivo riavvio del dispositivo.

È possibile aggiornare il firmware selezionato su un massimo di 50 dispositivi alla volta. Se si sceglie di aggiornare il firmware su più di 50 dispositivi selezionati, i dispositivi restanti vengono messi in coda. Un dispositivo in coda viene rimosso dalla coda di "aggiornamento del firmware selezionato" quando l'attivazione viene completata su un dispositivo aggiornato oppure quando un dispositivo aggiornato viene posizionato nello stato Modalità di manutenzione in sospeso (se è richiesto un riavvio su tale dispositivo). Quando un dispositivo che si trova nello stato Modalità di manutenzione in sospeso viene riavviato, il dispositivo si avvia in Modalità di manutenzione e continua il processo di aggiornamento, anche se il numero massimo di aggiornamenti firmware è già stato raggiunto.

È possibile aggiornare il firmware in bundle su un massimo di 10 dispositivi alla volta. Se si sceglie di aggiornare il firmware in bundle su più di 10 dispositivi, i dispositivi restanti vengono messi in coda. Un dispositivo in coda viene rimosso dalla coda di "aggiornamento firmware in bundle" al termine dell'attivazione di un dispositivo su cui è stato eseguito un aggiornamento firmware in bundle.

Attenzione: Per Red Hat® Enterprise Linux (RHEL) v7 e versioni successive, riavviare il sistema operativo da una modalità grafica consente di sospendere il server per impostazione predefinita. Prima di poter eseguire le azioni **Riavvia normalmente** o **Riavvia immediatamente** da XClarity Administrator, è necessario configurare manualmente il sistema operativo per modificare il comportamento del pulsante di alimentazione

su Spegni. Per istruzioni, vedere Guida di amministrazione e migrazione dei dati di Red Hat: modifica del comportamento in caso di pressione del pulsante di alimentazione in modalità di destinazione grafica.

Nota: XClarity Administrator abilita automaticamente l'interfaccia LAN-over-USB.

Applicazione degli aggiornamenti firmware in bundle utilizzando i criteri di conformità

Se Lenovo XClarity Administrator identifica un dispositivo gestito come non conforme, è possibile applicare manualmente gli aggiornamenti firmware a *tutti* i componenti dei server ThinkSystem SR635 e SR655 selezionati che non sono conformi ai criteri di conformità del firmware assegnati, utilizzando un'immagine in bundle che contiene i pacchetti di aggiornamento firmware applicabili. L'*immagine in bundle* viene creata durante il processo di aggiornamento raccogliendo tutti i pacchetti di aggiornamento firmware dai criteri di conformità.

Prima di iniziare

- Leggere le considerazioni sull'aggiornamento del firmware prima di tentare di aggiornare il firmware sui dispositivi gestiti (vedere Considerazioni sugli aggiornamenti firmware).
- Inizialmente, i dispositivi non supportati dagli aggiornamenti non vengono visualizzati. Non è possibile selezionare i dispositivi non supportati dagli aggiornamenti.
- Per impostazione predefinita, tutti i componenti rilevati sono elencati come disponibili per l'applicazione degli aggiornamenti; tuttavia, la presenza di firmware di livello inferiore potrebbe far sì che un componente non venga visualizzato nell'inventario o non presenti informazioni complete sulla versione. Per visualizzare l'elenco di tutti i pacchetti basati su criteri disponibili per l'applicazione di aggiornamenti, fare clic sull'icona **Tutte le azioni → Impostazioni globali** e selezionare **Supporto potenziato per dispositivi di livello inferiore**. Quando questa opzione è selezionata, la voce "Altro software disponibile" è riportata nella colonna Versione installata per i dispositivi non rilevati. Per ulteriori informazioni, vedere Configurazione delle impostazioni globali di aggiornamento del firmware.

  Nota:

  – Le impostazioni globali non possono essere modificate se sono in corso aggiornamenti ai dispositivi gestiti.

  – La generazione delle opzioni aggiuntive richiede alcuni minuti. Dopo alcune informazioni, potrebbe essere necessario fare clic sull'icona **Aggiorna** ( ) per aggiornare la tabella.
- Verificare che nessun processo sia attualmente in esecuzione sul server di destinazione. Se sono in esecuzione dei processi, il processo di aggiornamento viene messo in coda fino al completamento di tutti gli altri processi. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio → Processi**.
- L'applicazione degli aggiornamenti firmware in bundle è supportata solo per i server ThinkSystem SR635 e SR655.
- L'applicazione di aggiornamenti firmware in bundle è supportata solo per l'indirizzo IPv4. Gli indirizzi IPv6 non sono supportati.
- Verificare che ciascun dispositivo di destinazione sia stato avviato nel sistema operativo almeno una volta per recuperare le informazioni complete dell'inventario.
- Per utilizzare la funzione di aggiornamento in bundle è richiesto il firmware del controller di gestione della scheda di base v2.94 o versione successiva.
- Vengono utilizzati solo gli aggiornamenti firmware dei pacchetti del repository o i singoli aggiornamenti firmware. I pacchetti UpdateXpress System Packs (UXSPs) non sono supportati.
- Solo gli aggiornamenti firmware scaricati vengono applicati. Aggiornare il catalogo prodotti e scaricare gli aggiornamenti firmware appropriati (vedere Aggiornamento del catalogo prodotti e Download degli aggiornamenti firmware).

Nota: Quando XClarity Administrator viene installato per la prima volta, il catalogo prodotti e il repository sono vuoti.

- Il controllo di conformità è supportato solo per il controller di gestione della scheda di base e UEFI nei server ThinkSystem SR635 e SR655. XClarity Administrator tenta comunque di applicare gli aggiornamenti firmware a tutti i componenti hardware disponibili.
- Gli aggiornamenti vengono applicati in base ai criteri di conformità del firmware assegnati. Non è possibile scegliere di aggiornare un sottoinsieme di componenti.
- XClarity Administrator v3.2 o versione successiva è richiesto per applicare gli aggiornamenti firmware per Lenovo XClarity Provisioning Manager (LXPM), i driver Windows LXPM o i driver Linux LXPM ai server ThinkSystem SR635 e SR655.
- Gli aggiornamenti del controller di gestione della scheda di base e UEFI vengono ignorati se la versione attualmente installata è superiore ai criteri di conformità assegnati.
- I criteri di conformità del firmware devono essere creati e assegnati ai dispositivi ai quali si desidera applicare gli aggiornamenti firmware. Per ulteriori informazioni, vedere Creazione e assegnazione di criteri di conformità del firmware.
- I dispositivi selezionati verranno spenti prima di avviare il processo di aggiornamento. Verificare che qualsiasi carico di lavoro in esecuzione venga interrotto oppure, se si lavora in un ambiente virtualizzato, venga spostato su un server differente.

Attenzione: I dispositivi selezionati verranno spenti prima di avviare il processo di aggiornamento. Verificare che qualsiasi carico di lavoro in esecuzione venga interrotto oppure, se si lavora in un ambiente virtualizzato, venga spostato su un server differente. Se sono in esecuzione dei processi, il processo di aggiornamento viene messo in coda fino al completamento di tutti gli altri processi. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio → Processi**.

Informazioni su questa attività

Il processo di aggiornamento in bundle aggiorna innanzitutto il controller di gestione della scheda di base e UEFI fuori banda. Al termine degli aggiornamenti, il processo crea un'immagine in bundle del firmware restante nei criteri di conformità in base al tipo di macchina. Quindi, il processo monta l'immagine sul dispositivo selezionato e riavvia il dispositivo per avviare l'immagine. L'immagine viene eseguita automaticamente per completare gli aggiornamenti rimanenti.

È possibile aggiornare il firmware in bundle su un massimo di 10 dispositivi alla volta. Se si sceglie di aggiornare il firmware in bundle su più di 10 dispositivi, i dispositivi restanti vengono messi in coda. Un dispositivo in coda viene rimosso dalla coda di "aggiornamento firmware in bundle" al termine dell'attivazione di un dispositivo su cui è stato eseguito un aggiornamento firmware in bundle.

Se si verifica un errore durante l'aggiornamento di un componente nel dispositivo, il processo di aggiornamento firmware non aggiorna il firmware per quel componente specifico; tuttavia, il processo di aggiornamento firmware continua ad aggiornare gli altri componenti nel dispositivo e tutti gli altri dispositivi nel processo di aggiornamento firmware corrente.

Procedura

Per applicare gli aggiornamenti firmware sotto forma di immagine in bundle sui dispositivi gestiti, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Applica/Attiva**. Viene visualizzata la pagina Aggiornamenti firmware: Applica/Attiva.

Passo 2. Fare clic sulla scheda **Aggiorna con criteri**.

Passo 3. Selezionare uno o più dispositivi e componenti a cui devono essere applicati gli aggiornamenti firmware.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di dispositivi specifici. Inoltre, è possibile filtrare l'elenco dei dispositivi visualizzati, selezionando un'opzione nel menu **Mostra** per visualizzare solo i dispositivi in uno chassis, rack o gruppo specifico, immettendo il testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** oppure facendo clic sulle seguenti icone per visualizzare solo i dispositivi con uno stato specifico.

- Icona **Nascondi dispositivi conformi** ()
- Icona **Nascondi stato dispositivi non conformi** ()
- Icona **Nascondi dispositivi senza criteri di conformità assegnati** ()
- Icona **Nascondi i dispositivi non monitorati** ()
- Icona **Nascondi i dispositivi con attivazione firmware in sospeso** ()
- Icona **Nascondi i dispositivi con errori di conformità** ()
- Icona **Nascondi dispositivi non supportati per gli aggiornamenti** ()
- Icona **Nascondi dispositivi con aggiornamenti firmware in corso** ()
- Icona **Nascondi i dispositivi con firmware non temporaneo** ()

La colonna **Gruppi** indica i gruppi di cui ciascun dispositivo è membro. Passare il mouse sulla colonna **Gruppi** per ottenere un elenco completo dei gruppi, visualizzati per tipo di gruppo

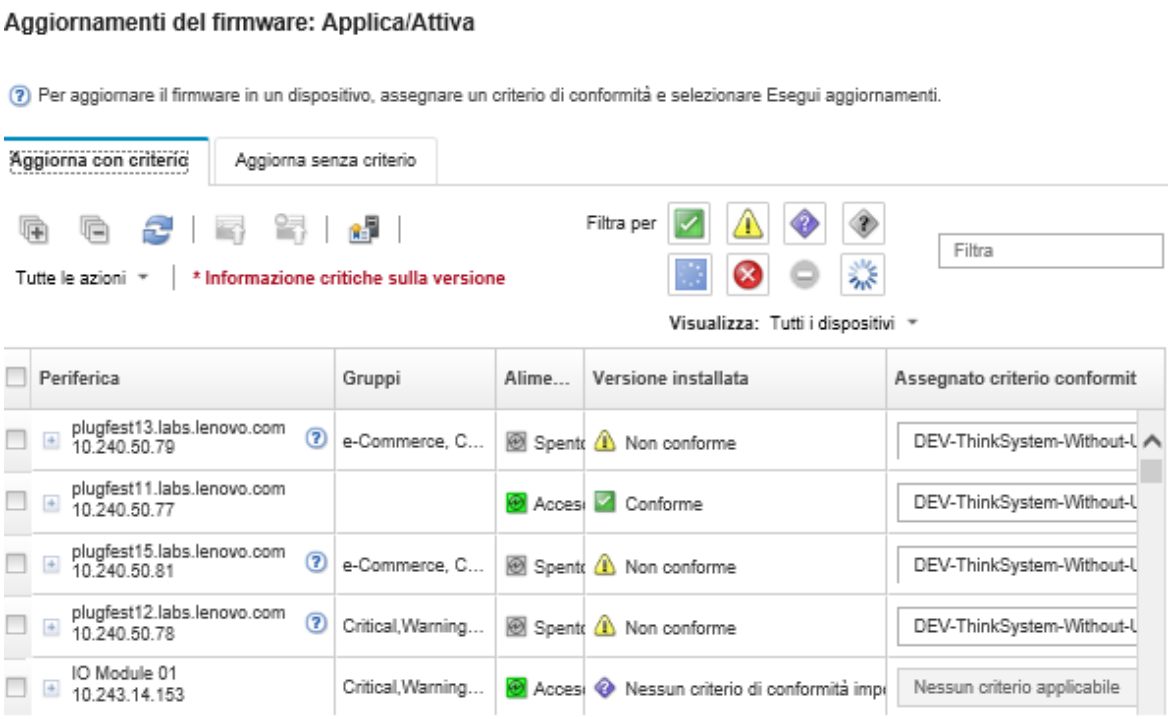
La colonna **Versione installata** indica la versione di firmware installata, lo stato della conformità o lo stato del dispositivo.

Lo stato della conformità può essere:

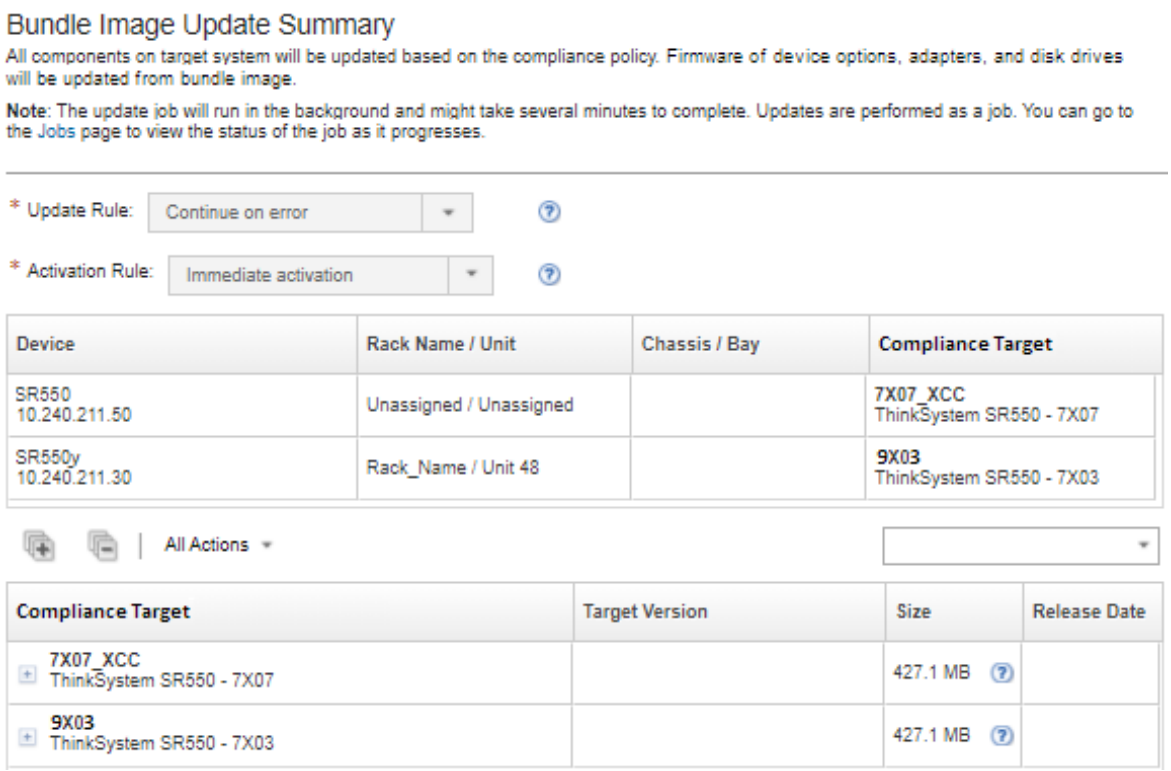
-  **Conforme**
-  **Errore di conformità**
-  **Non conforme**
-  **Nessun criterio di conformità impostato**
-  **Non monitorato**

Lo stato del dispositivo può essere:

-  **Aggiornamenti non supportati**
-  **Aggiornamento in corso**



Passo 4. Fare clic sull'icona **Esegui aggiornamento dall'immagine bundle** ( ). Viene visualizzata la finestra di dialogo Riepilogo aggiornamento immagine bundle. Questa finestra di dialogo elenca i dispositivi selezionati e gli aggiornamenti firmware inclusi nell'immagine in bundle.



Passo 5. Fare clic su **Esegui aggiornamento dall'immagine bundle** per eseguire subito l'aggiornamento oppure fare clic su **Pianifica** per pianificare l'esecuzione di questo aggiornamento in un secondo momento.

Al termine

Quando si applica un aggiornamento firmware, se il server non entra in modalità di manutenzione, tentare di applicare nuovamente l'aggiornamento.

Se gli aggiornamenti non sono stati completati correttamente, vedere Problemi del repository e dell'aggiornamento firmware nella documentazione online di XClarity Administrator per la risoluzione dei problemi e le azioni correttive.

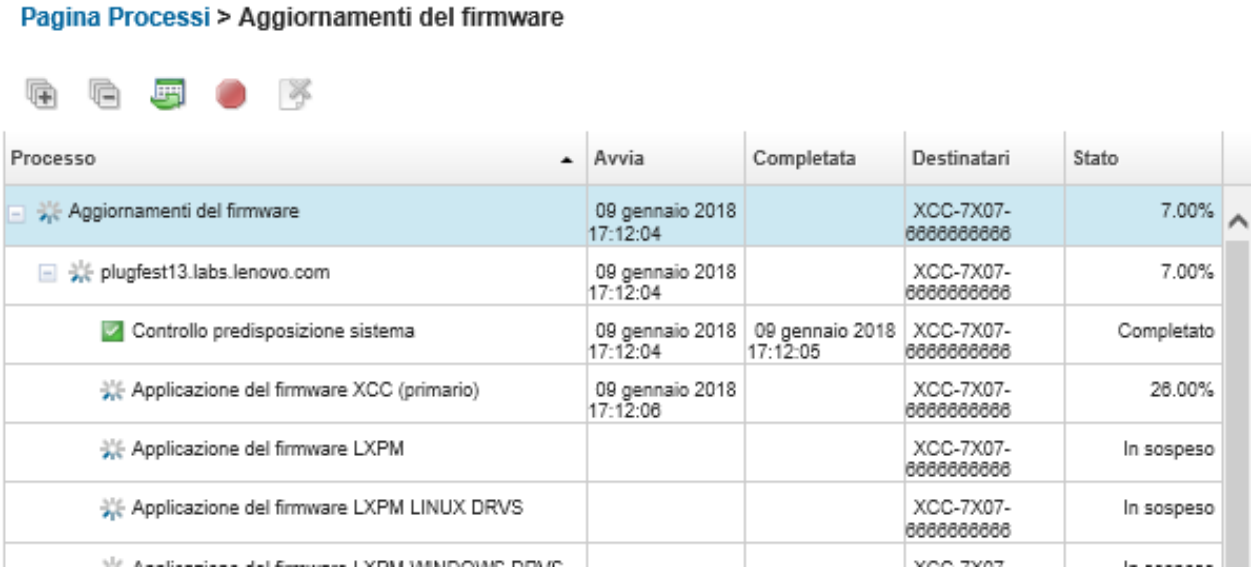
Dalla pagina Aggiornamenti firmware: Applica/Attiva è possibile eseguire le seguenti azioni.

- Esportare il firmware e le informazioni di conformità per ogni dispositivo gestito facendo clic su **Tutte le azioni → Esporta vista come CSV**.

  Nota: Il file CSV contiene solo le informazioni filtrate nella vista corrente. Non sono incluse le informazioni escluse dalla vista e quelle presenti nelle colonne nascoste.
- Annullare un aggiornamento applicato a un dispositivo selezionando il dispositivo e facendo clic sull'icona **Annulla aggiornamento** ( ).

  Nota: È possibile annullare gli aggiornamenti firmware in coda. Una volta avviato il processo di aggiornamento, l'aggiornamento del firmware può essere annullato solo quando il processo di aggiornamento sta eseguendo un'attività diversa da quella di applicazione dell'aggiornamento, come il passaggio alla modalità di manutenzione o il riavvio del dispositivo.
- Visualizzare lo stato dell'aggiornamento firmware direttamente dalla pagina Applica/Attiva nella colonna **Stato**.
- Monitorare lo stato del processo di aggiornamento dal log dei processi. Dal menu Lenovo XClarity Administrator, fare clic su **Monitoraggio → Processi**.

  Per ulteriori informazioni sul log dei processi, vedere Monitoraggio dei processi.



Una volta completati i processi di aggiornamento del firmware, è possibile verificare la conformità dei dispositivi facendo clic su **Provisioning → Aggiornamenti firmware: Applica/Attiva** per tornare alla pagina Aggiornamenti firmware: Applica/Attiva e facendo clic qui sull'icona **Aggiorna** ( ). La versione del firmware attualmente attiva su ciascun dispositivo è elencata nella colonna **Versione installata**.

Applicazione degli aggiornamenti firmware selezionati utilizzando i criteri di conformità

Dopo che Lenovo XClarity Administrator identifica un dispositivo come non conforme, è possibile applicare e attivare manualmente gli aggiornamenti firmware su tali dispositivi gestiti. È possibile scegliere di applicare e attivare tutti gli aggiornamenti firmware che si applicano ai criteri di conformità del firmware oppure solo gli aggiornamenti firmware specifici in un criterio. Solo gli aggiornamenti firmware scaricati vengono applicati.

Ulteriori informazioni:

- XClarity Administrator: aumento dell'efficenza durante l'aggiornamento del firmware
- Procedure ottimali per l'aggiornamento di driver e firmware di Lenovo ThinkSystem
- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: aggiornamenti firmware
- XClarity Administrator: provisioning degli aggiornamenti di sicurezza del firmware

Prima di iniziare

- Leggere le considerazioni sull'aggiornamento del firmware prima di tentare di aggiornare il firmware sui dispositivi gestiti (vedere Considerazioni sugli aggiornamenti firmware).
- Inizialmente, i dispositivi non supportati dagli aggiornamenti non vengono visualizzati. Non è possibile selezionare i dispositivi non supportati dagli aggiornamenti.
- Per impostazione predefinita, tutti i componenti rilevati sono elencati come disponibili per l'applicazione degli aggiornamenti; tuttavia, la presenza di firmware di livello inferiore potrebbe far sì che un componente non venga visualizzato nell'inventario o non presenti informazioni complete sulla versione. Per visualizzare l'elenco di tutti i pacchetti basati su criteri disponibili per l'applicazione di aggiornamenti, fare clic sull'icona **Tutte le azioni → Impostazioni globali** e selezionare **Supporto potenziato per dispositivi di livello inferiore**. Quando questa opzione è selezionata, la voce "Altro software disponibile" è riportata nella colonna Versione installata per i dispositivi non rilevati. Per ulteriori informazioni, vedere Configurazione delle impostazioni globali di aggiornamento del firmware.

  Nota:

  – Le impostazioni globali non possono essere modificate se sono in corso aggiornamenti ai dispositivi gestiti.

  – La generazione delle opzioni aggiuntive richiede alcuni minuti. Dopo alcune informazioni, potrebbe essere necessario fare clic sull'icona **Aggiorna** ( ) per aggiornare la tabella.
- Verificare che nessun processo sia attualmente in esecuzione sul server di destinazione. Se sono in esecuzione dei processi, il processo di aggiornamento viene messo in coda fino al completamento di tutti gli altri processi. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio → Processi**.
- Accertarsi che il repository degli aggiornamenti firmware contenga i pacchetti del firmware che si intende distribuire. In caso contrario, aggiornare il catalogo prodotti e scaricare gli aggiornamenti firmware appropriati (vedere Aggiornamento del catalogo prodotti e Download degli aggiornamenti firmware).

  Nota: Quando XClarity Administrator viene installato per la prima volta, il catalogo prodotti e il repository sono vuoti.

  Se si desidera installare il firmware prerequisito, assicurarsi che anch'esso sia stato scaricato nel repository.

  In alcuni casi, potrebbero essere necessarie più versioni per aggiornare il firmware e tutte le versioni devono essere scaricate nel repository. Ad esempio, per aggiornare lo switch scalabile IBM FC5022 SAN dalla versione 7.4.0a alla versione 8.2.0a, è necessario installare prima le versioni 8.0.1-pha e 8.1.1 e quindi la versione 8.2.0a. Per aggiornare lo switch alla versione 8.2.0a, tutte e tre le versioni devono essere state scaricate nel repository.

- In genere, per attivare gli aggiornamenti firmware occorre riavviare i dispositivi. Se si sceglie di riavviare il dispositivo durante il processo di aggiornamento (*attivazione immediata*), accertarsi che tutti i carichi di lavoro in esecuzione siano stati arrestati oppure, se si sta lavorando in un ambiente virtualizzato, siano stati spostati su un server diverso.
- Per i server ThinkSystem SR635 e SR655 è possibile utilizzare questa funzione di aggiornamento tradizionale per applicare solo gli aggiornamenti firmware del controller di gestione della scheda di base e gli aggiornamenti firmware UEFI. È necessario utilizzare la versione di firmware AMBT10M o successiva del controller di gestione ed è richiesta la versione di firmware UEFI CFE114L o successiva. Per aggiornare tutti i componenti (inclusi controller di gestione, UEFI, unità disco e opzioni I/O), utilizzare la funzione di aggiornamento bundle (vedere Applicazione degli aggiornamenti firmware in bundle utilizzando i criteri di conformità).

Informazioni su questa attività

- È possibile aggiornare il firmware selezionato su un massimo di 50 dispositivi alla volta. Se si sceglie di aggiornare il firmware su più di 50 dispositivi selezionati, i dispositivi restanti vengono messi in coda. Un dispositivo in coda viene rimosso dalla coda di "aggiornamento del firmware selezionato" quando l'attivazione viene completata su un dispositivo aggiornato oppure quando un dispositivo aggiornato viene posizionato nello stato Modalità di manutenzione in sospeso (se è richiesto un riavvio su tale dispositivo). Quando un dispositivo che si trova nello stato Modalità di manutenzione in sospeso viene riavviato, il dispositivo si avvia in Modalità di manutenzione e continua il processo di aggiornamento, anche se il numero massimo di aggiornamenti firmware è già stato raggiunto.
- È possibile applicare e attivare una versione firmware successiva a quella attualmente installata.
- È possibile scegliere di applicare tutti gli aggiornamenti per uno specifico dispositivo. Tuttavia, è anche possibile scegliere di espandere un dispositivo per specificare gli aggiornamenti per componenti specifici, quali il controller di gestione della scheda di base o UEFI.
- Se si sceglie di installare un pacchetto di aggiornamento firmware che contiene aggiornamenti per più componenti, vengono aggiornati tutti i componenti a cui viene applicato il pacchetto di aggiornamento.

Procedura

Per applicare e attivare gli aggiornamenti sui dispositivi gestiti, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Applica/Attiva**. Viene visualizzata la pagina Aggiornamenti firmware: Applica/Attiva.

Passo 2. Fare clic sulla scheda **Aggiorna con criteri**.

Passo 3. Selezionare uno o più dispositivi e i dispositivi cui devono essere applicati gli aggiornamenti firmware.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. Inoltre, è possibile filtrare l'elenco dei dispositivi visualizzati, selezionando un'opzione nel menu **Mostra** per visualizzare solo i dispositivi in uno chassis, rack o gruppo specifico, immettendo il testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** oppure facendo clic sulle seguenti icone per visualizzare solo i dispositivi con uno stato specifico.

- Icona **Nascondi dispositivi conformi** ()
- Icona **Nascondi stato dispositivi non conformi** ()
- Icona **Nascondi dispositivi senza criteri di conformità assegnati** ()
- Icona **Nascondi i dispositivi non monitorati** ()
- Icona **Nascondi i dispositivi con attivazione firmware in sospeso** ()

- Icona **Nascondi i dispositivi con errori di conformità** ()
- Icona **Nascondi dispositivi non supportati per gli aggiornamenti** ()
- Icona **Nascondi dispositivi con aggiornamenti firmware in corso** ()
- Icona **Nascondi i dispositivi con firmware non temporaneo** ()

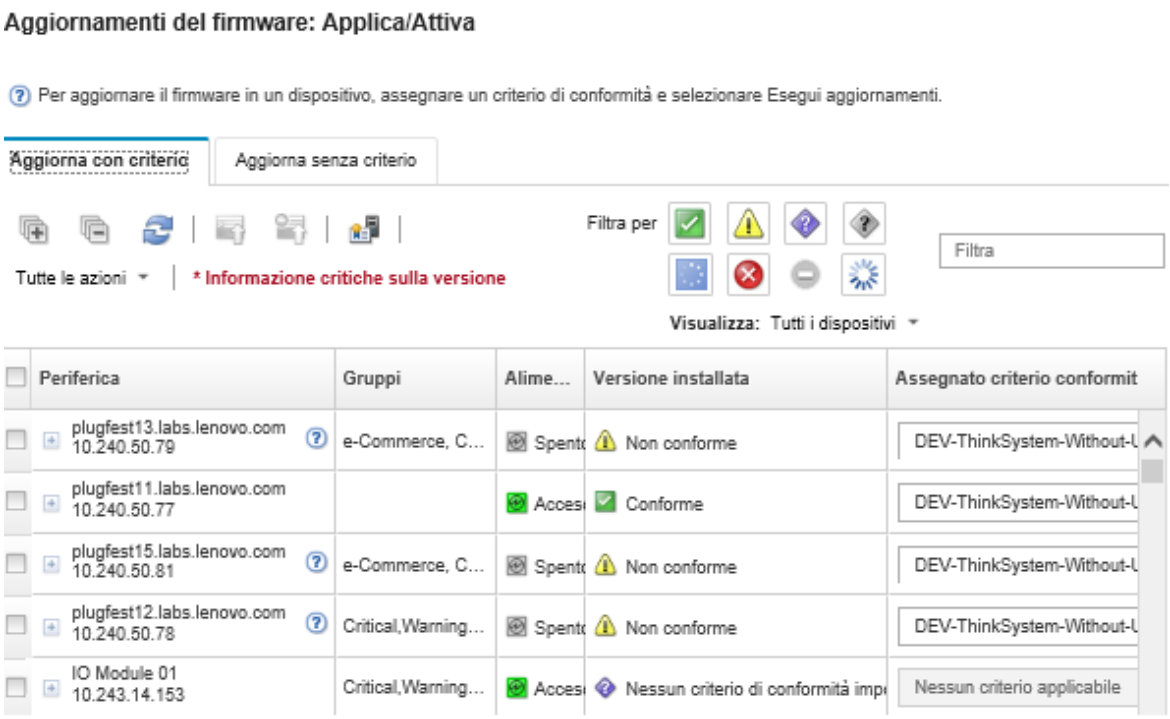
La colonna **Gruppi** indica i gruppi di cui ciascun dispositivo è membro. Passare il mouse sulla colonna **Gruppi** per ottenere un elenco completo dei gruppi, visualizzati per tipo di gruppo

La colonna **Versione installata** indica la versione di firmware installata, lo stato della conformità o lo stato del dispositivo.

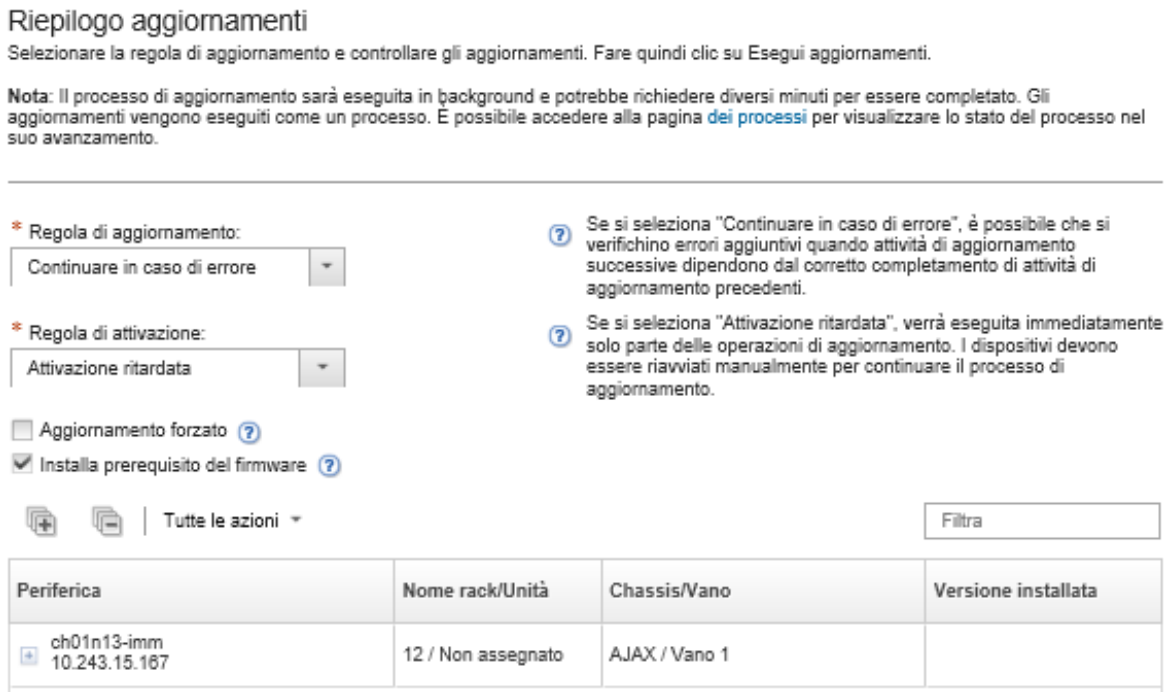
Lo stato della conformità può essere:
-  **Conforme**
-  **Errore di conformità**
-  **Non conforme**
-  **Nessun criterio di conformità impostato**
-  **Non monitorato**

Lo stato del dispositivo può essere:
-  **Aggiornamenti non supportati**
-  **Aggiornamento in corso**

Nota: Se la versione del firmware installato è in attesa di attivazione, la dicitura "(Attivazione in sospeso)" viene aggiunta alla versione di firmware installata o allo stato di conformità di ogni dispositivo applicabile, ad esempio "2.20 / A9E12EUS (Attivazione in sospeso)." Per visualizzare lo stato dell'attivazione in sospeso, è necessario installare la seguente versione del firmware sul controller di gestione della scheda di base primario del server.
- **IMM2**: TCOO46F, TCOO46E o versioni successive (a seconda della piattaforma)
- **XCC**: CDI328M, PSI316N, TEI334I o versioni successive (a seconda della piattaforma)



Passo 4. Fare clic sull'icona **Esegui aggiornamenti** ( ). Viene visualizzata la finestra di dialogo Riepilogo aggiornamenti.



Passo 5. Selezione di una delle seguenti regole di aggiornamento

- **Interrompi tutti gli aggiornamenti in caso di errore**. Se si verifica un errore durante l'aggiornamento dei componenti (come un adattatore o un controller di gestione) nel dispositivo di destinazione, il processo di aggiornamento firmware viene interrotto per tutti i dispositivi selezionati nel processo di aggiornamento firmware corrente. In questo caso, nessuno degli aggiornamenti nel pacchetto di aggiornamento del dispositivo viene applicato. Il firmware attuale installato su tutti i sistemi selezionati rimane valido.

- **Continua in caso di errore**. Se si verifica un errore durante l'aggiornamento di uno dei dispositivi nel dispositivo, il processo di aggiornamento firmware non aggiorna il firmware per quel dispositivo specifico; tuttavia, il processo di aggiornamento firmware continua ad aggiornare gli altri dispositivi nel dispositivo come pure tutti gli altri dispositivi nel processo di aggiornamento firmware corrente.
- **Continuare con il sistema successivo durante un errore**. Se si verifica un errore durante l'aggiornamento di uno dei dispositivi nel dispositivo, il processo di aggiornamento del firmware interrompe ogni tentativo di aggiornare il firmware per quel dispositivo specifico, in modo che il firmware attualmente installato nel dispositivo continui ad essere operativo. Il processo di aggiornamento firmware continuerà ad aggiornare tutti gli altri dispositivi nel processo di aggiornamento firmware corrente.

Passo 6. Selezionare una delle seguenti regole di attivazione:

- **Attivazione immediata** Durante il processo di aggiornamento, il dispositivo potrebbe essere riavviato automaticamente diverse volte finché l'intero processo di aggiornamento non viene completato. Accertarsi di sospendere tutte le applicazioni sul dispositivo prima di procedere.
- **Attivazione ritardata**. Alcune ma non tutte le operazioni di aggiornamento sono state eseguite. I dispositivi devono essere riavviati per continuare il processo di aggiornamento. Riavvii aggiuntivi vengono quindi eseguiti fino a che l'operazione di aggiornamento non è completa.

  Un evento si verifica quando lo stato viene modificato in **Modalità di manutenzione firmware in sospeso** per notificare quando il server deve essere riavviato.

  Se un dispositivo viene riavviato per un qualsiasi motivo, il processo di aggiornamento ritardato viene terminato.

  Questa regola di attivazione è supportata solo per i server e gli switch rack. I CMM e gli switch Flex vengono immediatamente attivati, indipendentemente da questa impostazione.

  Un evento si verifica quando lo stato viene modificato in **Modalità di manutenzione firmware in sospeso** per notificare quando il server deve essere riavviato.

  Il processo di aggiornamento ritardato viene completato quando il dispositivo viene riavviato per un qualsiasi motivo (incluso un riavvio manuale). Non sono previsti limiti di tempo per il riavvio del server.

  XClarity Administrator può applicare gli aggiornamenti con attivazione ritardata per un massimo di 50 dispositivi alla volta. Se si tenta di applicare gli aggiornamenti con attivazione ritardata per più di 50 dispositivi, i dispositivi restanti vengono messi in coda. Un dispositivo viene eliminato dalla coda quando in fase di aggiornamento viene posizionato nello stato **Modalità di manutenzione firmware in sospeso**.

  Importante:

  – Se XClarity Administrator viene riavviato durante il processo di aggiornamento, questo verrà interrotta con un errore.

  – Se un server che si trova nello stato **Modalità di manutenzione firmware in sospeso** viene riavviato mentre XClarity Administrator non è disponibile o raggiungibile, il server si avvia in modalità BMU, ma dato che XClarity Administrator non può collegarsi alla BMU e va in timeout dopo 60 secondi, lo stato di alimentazione del sistema viene ripristinato dal controller di gestione della scheda di base (si spegne se era spento, si riavvia se era acceso).
- **Attivazione con priorità**. Gli aggiornamenti firmware sul controller di gestione della scheda di base vengono attivati immediatamente; tutti gli altri aggiornamenti firmware vengono attivati al successivo riavvio del dispositivo. Riavvii aggiuntivi vengono quindi eseguiti fino a che l'operazione di aggiornamento non è completa. Questa regola è supportata solo per i server.

Un evento si verifica quando lo stato viene modificato in Modalità di manutenzione firmware in sospeso per notificare quando il server deve essere riavviato.

Nota: Se abilitata, l'opzione di avvio WOL (Wake-on-LAN) può interferire con le operazioni di XClarity Administrator che spengono il server, inclusi gli aggiornamenti firmware se nella rete è presente un client Wake-on-LAN che genera comandi "Magic Packet per riattivazione".

Passo 7. **Facoltativo:** selezionare **Forza aggiornamento** per aggiornare il firmware nei componenti selezionati anche se il livello di firmware è già aggiornato oppure per applicare un aggiornamento del firmware precedente a quello attualmente installato sui componenti installati.

Nota: È possibile applicare la versione precedente di firmware a opzioni di dispositivo, adattatori e unità che supportano l'abbassamento del livello. Consultare la documentazione hardware per determinare se è supportato il livello inferiore.

Passo 8. **Facoltativo:** deselezionare **Installa firmware prerequisito** se non si desidera installare il firmware prerequisito. Il firmware prerequisito viene installato per impostazione predefinita.

Nota: Quando si utilizza **Attivazione ritardata** o **Attivazione con priorità** per gli aggiornamenti firmware prerequisiti, potrebbe essere necessario riavviare il server per attivare il firmware prerequisito. Al riavvio iniziale, gli aggiornamenti firmware rimanenti vengono installati utilizzando **Attivazione immediata**.

Passo 9. **Facoltativo:** se si seleziona **Attivazione immediata**, scegliere **Test di memoria** per eseguire un test di memoria al termine dell'aggiornamento firmware, se il server viene riavviato durante l'aggiornamento.

Questa opzione è supportata per i server ThinkSystem v1 e v2 (esclusi i server ThinkSystem SR635, SR645, SR655 e SR665).

Passo 10. Fare clic su **Esegui aggiornamento** per eseguire subito l'aggiornamento oppure fare clic su **Pianifica** per pianificare l'esecuzione di questo aggiornamento in un secondo momento.

Se necessario, è possibile eseguire azioni di alimentazione sui dispositivi gestiti. Le azioni di alimentazione sono utili quando è selezionato **Attivazione ritardata** e si desidera che gli aggiornamenti continuino quando il dispositivo è in attesa nello stato "In attesa di manutenzione". Per eseguire un'azione di alimentazione su un dispositivo gestito da questa pagina, fare clic su **Tutte le azioni → Azioni di alimentazione**, quindi fare clic su una delle seguenti azioni di alimentazione.

- **Accendi**
- **Arresta sistema operativo e spegni**
- **Spegni**
- **Arresta sistema operativo e riavvia**
- **Riavvia**

Al termine

Quando si applica un aggiornamento firmware, se il server non entra in modalità di manutenzione, tentare di applicare nuovamente l'aggiornamento.

Se gli aggiornamenti non sono stati completati correttamente, vedere Problemi del repository e dell'aggiornamento firmware nella documentazione online di XClarity Administrator per la risoluzione dei problemi e le azioni correttive.

Dalla pagina "Aggiornamenti firmware: Applica/Attiva" è possibile eseguire le seguenti azioni:

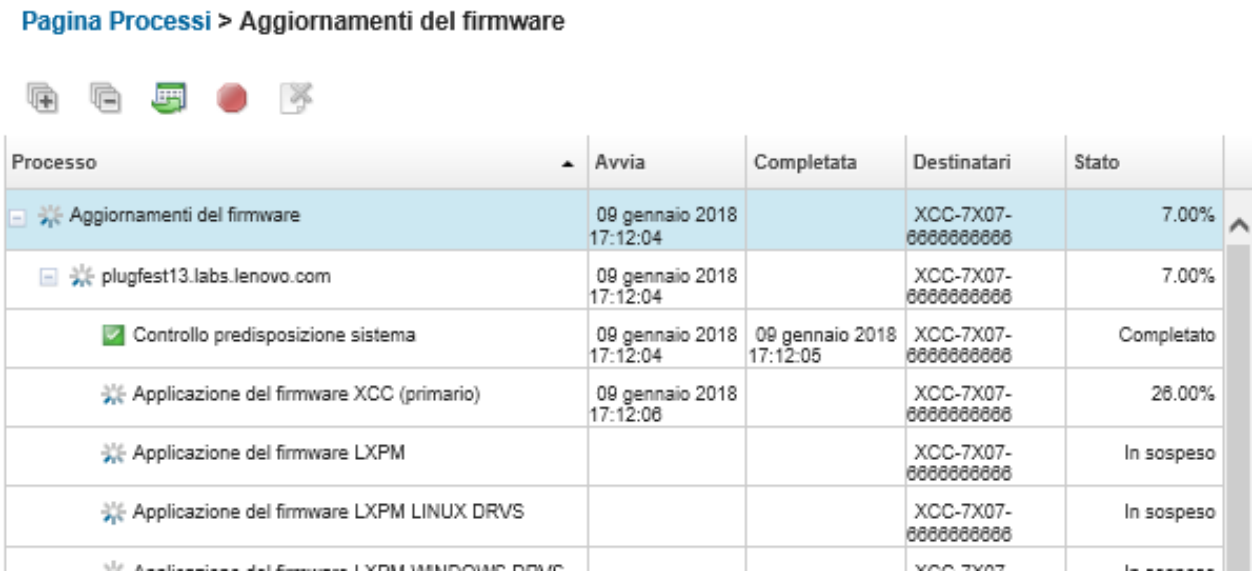
- Esportare il firmware e le informazioni di conformità per ogni dispositivo gestito facendo clic su **Tutte le azioni → Esporta vista come CSV**.

Nota: Il file CSV contiene solo le informazioni filtrate nella vista corrente. Non sono incluse le informazioni escluse dalla vista e quelle presenti nelle colonne nascoste.

- Annullare un aggiornamento applicato a un dispositivo selezionando il dispositivo e facendo clic sull'icona **Annulla aggiornamento** ( ).

  Nota: È possibile annullare gli aggiornamenti firmware in coda. Una volta avviato il processo di aggiornamento, l'aggiornamento del firmware può essere annullato solo quando il processo di aggiornamento sta eseguendo un'attività diversa da quella di applicazione dell'aggiornamento, come il passaggio alla modalità di manutenzione o il riavvio del dispositivo.
- Visualizzare lo stato dell'aggiornamento firmware direttamente dalla pagina Applica/Attiva nella colonna **Stato**.
- Monitorare lo stato del processo di aggiornamento dal log dei processi. Dal menu Lenovo XClarity Administrator, fare clic su **Monitoraggio → Processi**.

  Per ulteriori informazioni sul log dei processi, vedere Monitoraggio dei processi.



  Una volta completati i processi di aggiornamento del firmware, è possibile verificare la conformità dei dispositivi facendo clic su **Provisioning → Aggiornamenti firmware: Applica/Attiva** per tornare alla pagina Aggiornamenti firmware: Applica/Attiva e facendo clic qui sull'icona **Aggiorna** ( ). La versione del firmware attualmente attiva su ciascun dispositivo è elencata nella colonna **Versione installata**.

Applicazione degli aggiornamenti firmware selezionati senza utilizzare criteri di conformità

È possibile applicare e attivare rapidamente un firmware più aggiornato rispetto a quello attualmente installato su un singolo dispositivo o su un gruppo di dispositivi gestiti senza utilizzare i criteri di conformità.

Ulteriori informazioni:

- XClarity Administrator: aumento dell'efficenza durante l'aggiornamento del firmware
- Procedure ottimali per l'aggiornamento di driver e firmware di Lenovo ThinkSystem
- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: aggiornamenti firmware
- XClarity Administrator: provisioning degli aggiornamenti di sicurezza del firmware

Prima di iniziare

- Leggere le considerazioni sull'aggiornamento del firmware prima di tentare di aggiornare il firmware sui dispositivi gestiti (vedere Considerazioni sugli aggiornamenti firmware).
- Inizialmente, i dispositivi non supportati dagli aggiornamenti non vengono visualizzati. Non è possibile selezionare i dispositivi non supportati dagli aggiornamenti.
- Per impostazione predefinita, tutti i componenti rilevati sono elencati come disponibili per l'applicazione degli aggiornamenti; tuttavia, la presenza di firmware di livello inferiore potrebbe far sì che un componente non venga visualizzato nell'inventario o non presenti informazioni complete sulla versione. Per visualizzare l'elenco di tutti i pacchetti basati su criteri disponibili per l'applicazione di aggiornamenti, fare clic sull'icona **Tutte le azioni → Impostazioni globali** e selezionare **Supporto potenziato per dispositivi di livello inferiore**. Quando questa opzione è selezionata, la voce "Altro software disponibile" è riportata nella colonna Versione installata per i dispositivi non rilevati. Per ulteriori informazioni, vedere Configurazione delle impostazioni globali di aggiornamento del firmware.

  Nota:

  – Le impostazioni globali non possono essere modificate se sono in corso aggiornamenti ai dispositivi gestiti.

  – La generazione delle opzioni aggiuntive richiede alcuni minuti. Dopo alcune informazioni, potrebbe essere necessario fare clic sull'icona **Aggiorna** () per aggiornare la tabella.
- Verificare che nessun processo sia attualmente in esecuzione sul server di destinazione. Se sono in esecuzione dei processi, il processo di aggiornamento viene messo in coda fino al completamento di tutti gli altri processi. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio → Processi**.
- Accertarsi che il repository degli aggiornamenti firmware contenga i pacchetti del firmware che si intende distribuire. In caso contrario, aggiornare il catalogo prodotti e scaricare gli aggiornamenti firmware appropriati (vedere Aggiornamento del catalogo prodotti e Download degli aggiornamenti firmware).

  Nota: Quando XClarity Administrator viene installato per la prima volta, il catalogo prodotti e il repository sono vuoti.

  Se si desidera installare il firmware prerequisito, assicurarsi che anch'esso sia stato scaricato nel repository.

  In alcuni casi, potrebbero essere necessarie più versioni per aggiornare il firmware e tutte le versioni devono essere scaricate nel repository. Ad esempio, per aggiornare lo switch scalabile IBM FC5022 SAN dalla versione 7.4.0a alla versione 8.2.0a, è necessario installare prima le versioni 8.0.1-pha e 8.1.1 e quindi la versione 8.2.0a. Per aggiornare lo switch alla versione 8.2.0a, tutte e tre le versioni devono essere state scaricate nel repository.
- In genere, per attivare gli aggiornamenti firmware occorre riavviare i dispositivi. Se si sceglie di riavviare il dispositivo durante il processo di aggiornamento (*attivazione immediata*), accertarsi che tutti i carichi di lavoro in esecuzione siano stati arrestati oppure, se si sta lavorando in un ambiente virtualizzato, siano stati spostati su un server diverso.

Informazioni su questa attività

- È possibile aggiornare il firmware selezionato su un massimo di 50 dispositivi alla volta. Se si sceglie di aggiornare il firmware su più di 50 dispositivi selezionati, i dispositivi restanti vengono messi in coda. Un dispositivo in coda viene rimosso dalla coda di "aggiornamento del firmware selezionato" quando l'attivazione viene completata su un dispositivo aggiornato oppure quando un dispositivo aggiornato viene posizionato nello stato Modalità di manutenzione in sospeso (se è richiesto un riavvio su tale dispositivo). Quando un dispositivo che si trova nello stato Modalità di manutenzione in sospeso viene riavviato, il dispositivo si avvia in Modalità di manutenzione e continua il processo di aggiornamento, anche se il numero massimo di aggiornamenti firmware è già stato raggiunto.

- È possibile applicare e attivare una versione firmware successiva a quella attualmente installata.
- È possibile scegliere di applicare tutti gli aggiornamenti per uno specifico dispositivo. Tuttavia, è anche possibile scegliere di espandere un dispositivo per specificare gli aggiornamenti per componenti specifici, quali il controller di gestione della scheda di base o UEFI.
- Se si sceglie di installare un pacchetto di aggiornamento firmware che contiene aggiornamenti per più componenti, vengono aggiornati tutti i componenti a cui viene applicato il pacchetto di aggiornamento.

Procedura

Per applicare e attivare gli aggiornamenti su un dispositivo gestito, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti firmware: Applica/Attiva**. Viene visualizzata la pagina Aggiornamenti firmware: Applica/Attiva.

Passo 2. Fare clic sulla scheda **Aggiorna senza criteri**.

Passo 3. Selezionare il livello di firmware nella colonna **Versioni più recenti scaricate** per ciascun dispositivo da aggiornare.

Passo 4. Selezionare uno o più dispositivi e i dispositivi che si desidera aggiornare.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. Inoltre, è possibile filtrare l'elenco dei dispositivi visualizzati, selezionando un'opzione nel menu **Mostra** per visualizzare solo i dispositivi in uno chassis, rack o gruppo specifico, immettendo il testo (ad esempio, nome o indirizzo IP) nel campo **Filtro** oppure facendo clic sulle seguenti icone per visualizzare solo i dispositivi con uno stato specifico.

- Icona **Nascondi componenti con alcune versioni più recenti** ()
- Icona **Nascondi componenti senza versioni più recenti** ()
- Icona **Nascondi dispositivi non supportati per gli aggiornamenti** ()
- Icona **Nascondi dispositivi con aggiornamenti firmware in corso** ()
- Icona **Nascondi i dispositivi con firmware non temporaneo** ()

La colonna **Gruppi** indica i gruppi di cui ciascun dispositivo è membro. Passare il mouse sulla colonna **Gruppi** per ottenere un elenco completo dei gruppi, visualizzati per tipo di gruppo

La colonna **Versione installata** indica la versione di firmware installata, lo stato della conformità o lo stato del dispositivo.

Lo stato della conformità può essere:

-  **Conforme**
-  **Errore di conformità**
-  **Non conforme**
-  **Nessun criterio di conformità impostato**
-  **Non monitorato**

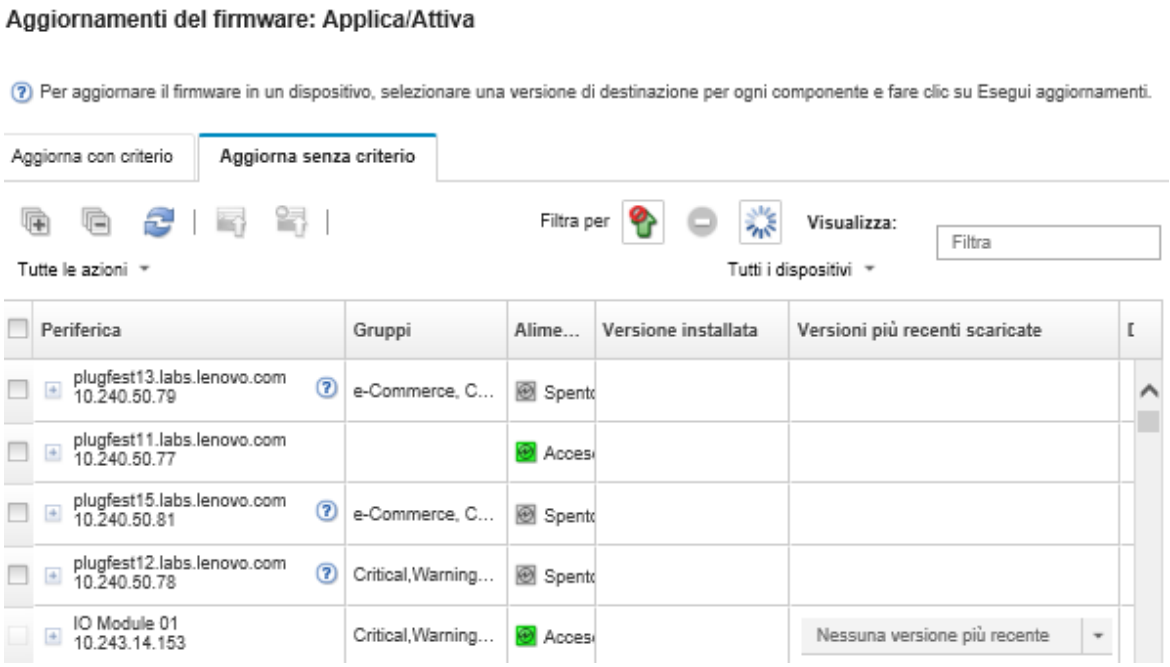
Lo stato del dispositivo può essere:

-  **Aggiornamenti non supportati**
-  **Aggiornamento in corso**

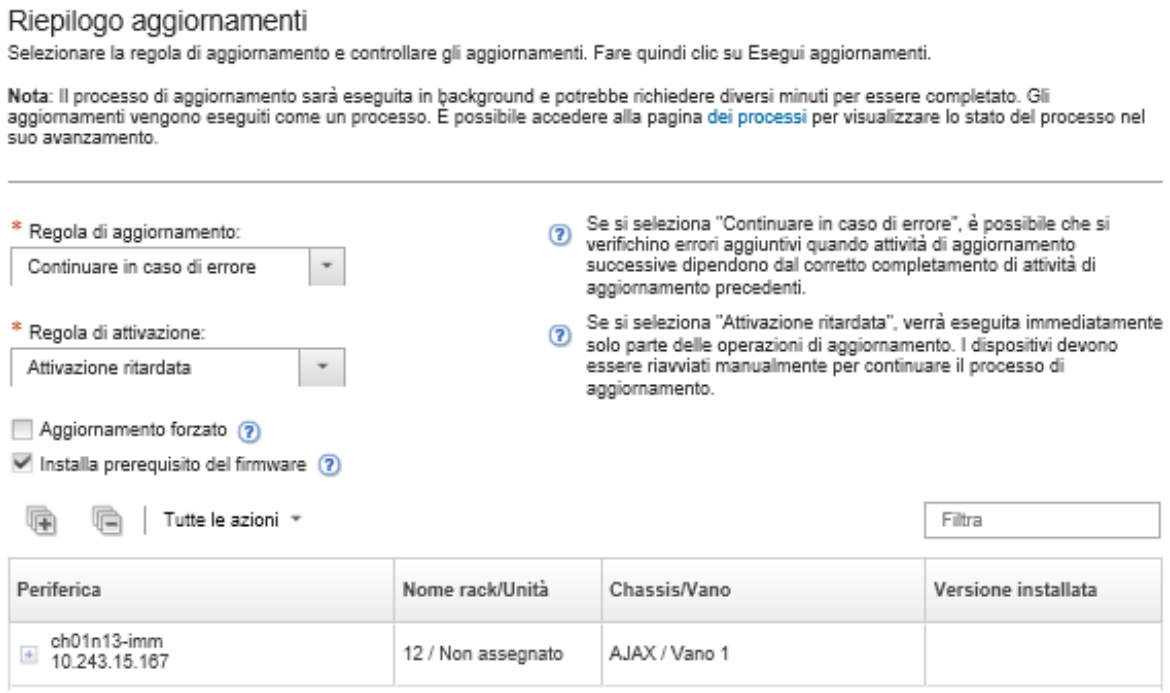
Nota: Se la versione del firmware installato è in attesa di attivazione, la dicitura "(Attivazione in sospeso)" viene aggiunta alla versione di firmware installata o allo stato di conformità di ogni

dispositivo applicabile, ad esempio "2.20 / A9E12EUS (Attivazione in sospeso)." Per visualizzare lo stato dell'attivazione in sospeso, è necessario installare la seguente versione del firmware sul controller di gestione della scheda di base primario del server.

- **IMM2**: TCOO46F, TCOO46E o versioni successive (a seconda della piattaforma)
- **XCC**: CDI328M, PSI316N, TEI334I o versioni successive (a seconda della piattaforma)



Passo 5. Fare clic sull'icona **Esegui aggiornamenti** ( ). Viene visualizzata la finestra di dialogo Riepilogo aggiornamenti.



Passo 6. Selezione di una delle seguenti regole di aggiornamento

- **Interrompi tutti gli aggiornamenti in caso di errore**. Se si verifica un errore durante l'aggiornamento dei componenti (come un adattatore o un controller di gestione) nel dispositivo di destinazione, il processo di aggiornamento firmware viene interrotto per tutti i dispositivi selezionati nel processo di aggiornamento firmware corrente. In questo caso, nessuno degli aggiornamenti nel pacchetto di aggiornamento del dispositivo viene applicato. Il firmware attuale installato su tutti i sistemi selezionati rimane valido.
- **Continua in caso di errore**. Se si verifica un errore durante l'aggiornamento di uno dei dispositivi nel dispositivo, il processo di aggiornamento firmware non aggiorna il firmware per quel dispositivo specifico; tuttavia, il processo di aggiornamento firmware continua ad aggiornare gli altri dispositivi nel dispositivo come pure tutti gli altri dispositivi nel processo di aggiornamento firmware corrente.
- **Continuare con il sistema successivo durante un errore**. Se si verifica un errore durante l'aggiornamento di uno dei dispositivi nel dispositivo, il processo di aggiornamento del firmware interrompe ogni tentativo di aggiornare il firmware per quel dispositivo specifico, in modo che il firmware attualmente installato nel dispositivo continui ad essere operativo. Il processo di aggiornamento firmware continuerà ad aggiornare tutti gli altri dispositivi nel processo di aggiornamento firmware corrente.

Nota: Se abilitata, l'opzione di avvio WOL (Wake-on-LAN) può interferire con le operazioni di XClarity Administrator che spengono il server, inclusi gli aggiornamenti firmware se nella rete è presente un client Wake-on-LAN che genera comandi "Magic Packet per riattivazione".

Passo 7. Selezionare una delle seguenti regole di attivazione:

- **Attivazione immediata** Durante il processo di aggiornamento, il dispositivo potrebbe essere riavviato automaticamente diverse volte finché l'intero processo di aggiornamento non viene completato. Accertarsi di sospendere tutte le applicazioni sul dispositivo prima di procedere.
- **Attivazione ritardata**. Alcune ma non tutte le operazioni di aggiornamento sono state eseguite. I dispositivi devono essere riavviati per continuare il processo di aggiornamento. Riavvii aggiuntivi vengono quindi eseguiti fino a che l'operazione di aggiornamento non è completa.

  Un evento si verifica quando lo stato viene modificato in **Modalità di manutenzione firmware in sospeso** per notificare quando il server deve essere riavviato.

  Se un dispositivo viene riavviato per un qualsiasi motivo, il processo di aggiornamento ritardato viene terminato.

  Questa regola di attivazione è supportata solo per i server e gli switch rack. I CMM e gli switch Flex vengono immediatamente attivati, indipendentemente da questa impostazione.

  Un evento si verifica quando lo stato viene modificato in **Modalità di manutenzione firmware in sospeso** per notificare quando il server deve essere riavviato.

  Il processo di aggiornamento ritardato viene completato quando il dispositivo viene riavviato per un qualsiasi motivo (incluso un riavvio manuale). Non sono previsti limiti di tempo per il riavvio del server.

  XClarity Administrator può applicare gli aggiornamenti con attivazione ritardata per un massimo di 50 dispositivi alla volta. Se si tenta di applicare gli aggiornamenti con attivazione ritardata per più di 50 dispositivi, i dispositivi restanti vengono messi in coda. Un dispositivo viene eliminato dalla coda quando in fase di aggiornamento viene posizionato nello stato **Modalità di manutenzione firmware in sospeso**.

  Importante:

  – Se XClarity Administrator viene riavviato durante il processo di aggiornamento, questo verrà interrotta con un errore.

– Se un server che si trova nello stato **Modalità di manutenzione firmware in sospeso** viene riavviato mentre XClarity Administrator non è disponibile o raggiungibile, il server si avvia in modalità BMU, ma dato che XClarity Administrator non può collegarsi alla BMU e va in timeout dopo 60 secondi, lo stato di alimentazione del sistema viene ripristinato dal controller di gestione della scheda di base (si spegne se era spento, si riavvia se era acceso).

- **Attivazione con priorità**. Gli aggiornamenti firmware sul controller di gestione della scheda di base vengono attivati immediatamente; tutti gli altri aggiornamenti firmware vengono attivati al successivo riavvio del dispositivo. Riavvii aggiuntivi vengono quindi eseguiti fino a che l'operazione di aggiornamento non è completa. Questa regola è supportata solo per i server.

  Un evento si verifica quando lo stato viene modificato in Modalità di manutenzione firmware in sospeso per notificare quando il server deve essere riavviato.

Nota: Se abilitata, l'opzione di avvio WOL (Wake-on-LAN) può interferire con le operazioni di XClarity Administrator che spengono il server, inclusi gli aggiornamenti firmware se nella rete è presente un client Wake-on-LAN che genera comandi "Magic Packet per riattivazione".

Passo 8. **Facoltativo:** selezionare **Forza aggiornamento** per aggiornare il firmware nei componenti selezionati anche se il livello di firmware è già aggiornato oppure per applicare un aggiornamento del firmware precedente a quello attualmente installato sui componenti installati.

Nota: È possibile applicare la versione precedente di firmware a opzioni di dispositivo, adattatori e unità che supportano l'abbassamento del livello. Consultare la documentazione hardware per determinare se è supportato il livello inferiore.

Passo 9. **Facoltativo:** deselezionare **Installa firmware prerequisito** se non si desidera installare il firmware prerequisito. Il firmware prerequisito viene installato per impostazione predefinita.

Nota: Quando si utilizza **Attivazione ritardata** o **Attivazione con priorità** per gli aggiornamenti firmware prerequisiti, potrebbe essere necessario riavviare il server per attivare il firmware prerequisito. Al riavvio iniziale, gli aggiornamenti firmware rimanenti vengono installati utilizzando **Attivazione immediata**.

Passo 10. **Facoltativo:** se si seleziona **Attivazione immediata**, scegliere **Test di memoria** per eseguire un test di memoria al termine dell'aggiornamento firmware, se il server viene riavviato durante l'aggiornamento.

Questa opzione è supportata per i server ThinkSystem v1 e v2 (esclusi i server ThinkSystem SR635, SR645, SR655 e SR665).

Passo 11. Fare clic su **Esegui aggiornamento** per eseguire subito l'aggiornamento oppure fare clic su **Pianifica** per pianificare l'esecuzione di questo aggiornamento in un secondo momento.

Se necessario, è possibile eseguire azioni di alimentazione sui dispositivi gestiti. Le azioni di alimentazione sono utili quando è selezionato **Attivazione ritardata** e si desidera che gli aggiornamenti continuino quando il dispositivo è in attesa nello stato "In attesa di manutenzione". Per eseguire un'azione di alimentazione su un dispositivo gestito da questa pagina, fare clic su **Tutte le azioni → Azioni di alimentazione**, quindi fare clic su una delle seguenti azioni di alimentazione.

- **Accendi**
- **Arresta sistema operativo e spegni**
- **Spegni**
- **Arresta sistema operativo e riavvia**
- **Riavvia**

Al termine

Quando si applica un aggiornamento firmware, se il server non entra in modalità di manutenzione, tentare di applicare nuovamente l'aggiornamento.

Se gli aggiornamenti non sono stati completati correttamente, vedere Problemi del repository e dell'aggiornamento firmware nella documentazione online di XClarity Administrator per la risoluzione dei problemi e le azioni correttive.

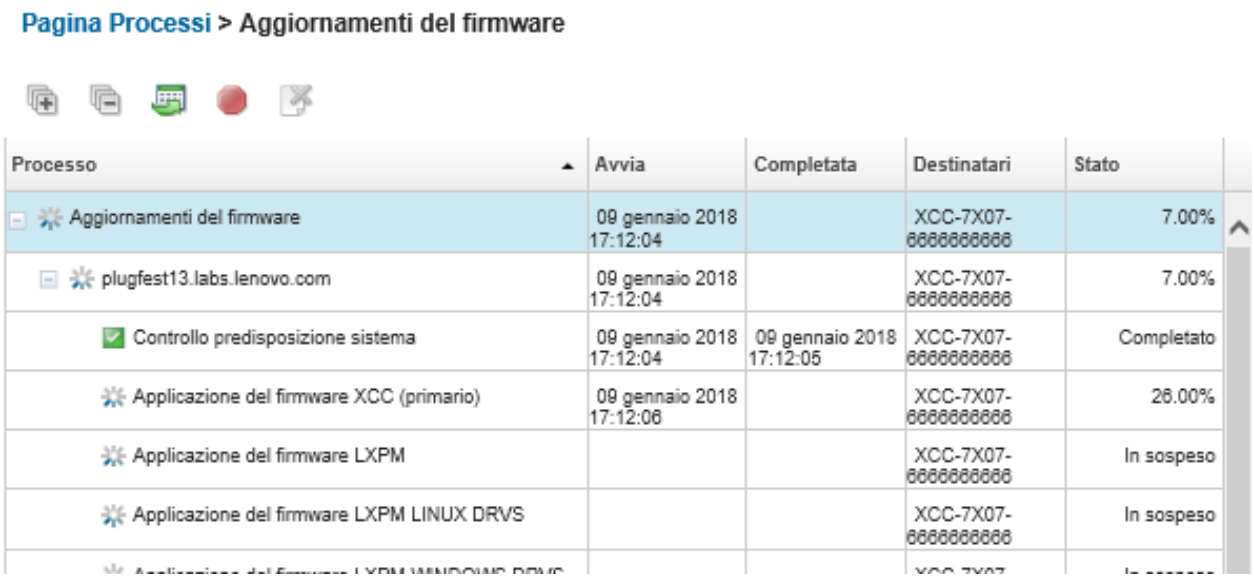
Dalla pagina "Aggiornamenti firmware: Applica/Attiva" è possibile eseguire le seguenti azioni:

- Esportare il firmware e le informazioni di conformità per ogni dispositivo gestito facendo clic su **Tutte le azioni → Esporta vista come CSV**.

  Nota: Il file CSV contiene solo le informazioni filtrate nella vista corrente. Non sono incluse le informazioni escluse dalla vista e quelle presenti nelle colonne nascoste.
- Annullare un aggiornamento applicato a un dispositivo selezionando il dispositivo e facendo clic sull'icona **Annulla aggiornamento** ( ).

  Nota: È possibile annullare gli aggiornamenti firmware in coda. Una volta avviato il processo di aggiornamento, l'aggiornamento del firmware può essere annullato solo quando il processo di aggiornamento sta eseguendo un'attività diversa da quella di applicazione dell'aggiornamento, come il passaggio alla modalità di manutenzione o il riavvio del dispositivo.
- Visualizzare lo stato dell'aggiornamento firmware direttamente dalla pagina Applica/Attiva nella colonna **Stato**.
- Monitorare lo stato del processo di aggiornamento dal log dei processi. Dal menu Lenovo XClarity Administrator, fare clic su **Monitoraggio → Processi**.

  Per ulteriori informazioni sul log dei processi, vedere Monitoraggio dei processi.



Una volta completati i processi di aggiornamento del firmware, è possibile verificare la conformità dei dispositivi facendo clic su **Provisioning → Aggiornamenti firmware: Applica/Attiva** per tornare alla pagina Aggiornamenti firmware: Applica/Attiva e facendo clic qui sull'icona **Aggiorna** ( ). La versione del firmware attualmente attiva su ciascun dispositivo è elencata nella colonna **Versione installata**.

Capitolo 14. Aggiornamento dei driver di dispositivo di Windows sui server gestiti

Utilizzando i pacchetti UpdateXpress System Packs (UXSPs) di Windows, è possibile aggiornare i driver di dispositivo del sistema operativo sui sistemi operativi Windows distribuiti.

Prima di iniziare

È necessario disporre dell'autorità **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** o **lxc-hw-admin** per gestire e distribuire i driver di dispositivo del sistema operativo, nonché per eseguire azioni di alimentazione sui server gestiti dalle pagine "Aggiornamenti dei driver di Windows".

L'aggiornamento del firmware e dei driver di dispositivo sono processi separati in XClarity Administrator; questi processi non sono in alcun modo connessi. XClarity Administrator non gestisce la conformità tra il firmware e i driver dei dispositivi sui dispositivi gestiti, anche se si consiglia di aggiornare i driver di dispositivo contemporaneamente al firmware.

Informazioni su questa attività

Windows UpdateXpress System Packs (UXSPs) contiene i driver di dispositivo per le versioni supportate di Windows e per i server Lenovo che supportano Windows.

Sono supportati solo i driver di dispositivo per Windows Server 2012 R2 e versioni successive. XClarity Administrator non supporta l'aggiornamento dei driver di dispositivo Linux o VMware.

Per informazioni sull'installazione dei driver di dispositivo durante la distribuzione dei sistemi operativi, vedere Installazione dei sistemi operativi sui server bare metal.

Procedura

Passo 1. **Configurazione di Windows Server per gli aggiornamenti dei driver di dispositivo del sistema operativo**

Lenovo XClarity Administrator utilizza il servizio Gestione remota Windows (WinRM) in ascolto su HTTPS o HTTP per eseguire i comandi di aggiornamento dei driver di dispositivo sui sistemi Windows di destinazione. Il servizio WinRM deve essere configurato correttamente sul server di destinazione prima di tentare di aggiornare i driver di dispositivo del sistema operativo (vedere Configurazione di Windows Server per gli aggiornamenti dei driver di dispositivo del sistema operativo).

Passo 2. **Gestione del repository dei driver di dispositivo del sistema operativo**

Il *repository dei driver di dispositivo del sistema operativo* contiene un catalogo di driver di dispositivo Windows disponibili e i pacchetti di driver di dispositivo che possono essere applicati ai dispositivi gestiti.

Il *catalogo* contiene informazioni su tutti i pacchetti UXSPs (UpdateXpress System Packs) e gli aggiornamenti dei driver di dispositivo di Windows, disponibili per tutti i server Lenovo che supportano Windows. Il catalogo organizza gli aggiornamenti dei driver di dispositivo per tipo di dispositivo. Quando si aggiorna il catalogo, XClarity Administrator recupera le informazioni sui pacchetti UXSP disponibili dal Sito Web dell'Assistenza del Centro Dati Lenovo (come i file metadata.xml e readme.txt) e memorizza le informazioni nel repository. Il file di payload (.exe) non è stato

scaricato. Per ulteriori informazioni sull'aggiornamento del catalogo, vedere Aggiornamento del catalogo dei driver di dispositivo del sistema operativo.

È possibile scaricare o importare gli UXSPs di Windows nel repository. I pacchetti UXSPs di Windows contengono i driver di dispositivo di WIndows per le versioni supportate di Windows e per i server Lenovo che supportano Windows. I pacchetti UXSPs devono essere disponibili nel repository prima che sia possibile aggiornare i driver di dispositivo di Windows sui server gestiti. Per ulteriori informazioni sul download dei driver di dispositivo, vedere Download dei driver di dispositivo di Windows .

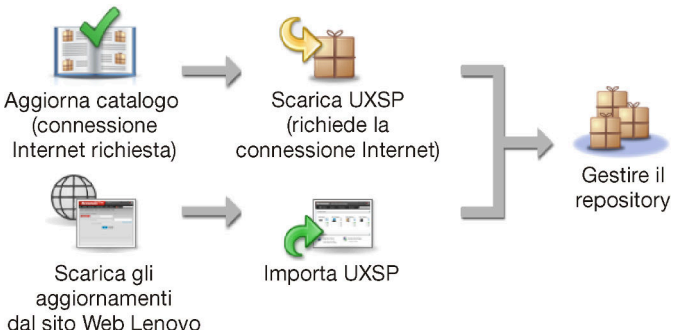
È possibile determinare se i pacchetti UXSPs vengono archiviati nel repository dei driver di dispositivo del sistema operativo dalla colonna Stato del download nella scheda Aggiornamenti individuali della pagina del repository Aggiornamenti dei driver di Windows. Questa colonna contiene i seguenti valori.

- **Scaricato**. L'intero pacchetto o il singolo aggiornamento viene archiviato nel repository.
- ***x* di *y* scaricati**. Non tutti gli aggiornamenti nel pacchetto vengono archiviati nel repository. I numeri tra parentesi indicano il numero di aggiornamenti disponibili e il numero di aggiornamenti memorizzati, oppure l'indisponibilità di aggiornamenti per il tipo di dispositivo specifico.
- **Non scaricato**. L'intero pacchetto o il singolo aggiornamento è disponibile, ma non viene archiviato nel repository.

Nota: Quando si scaricano o si importano i pacchetti UXSPs dalla pagina "Repository di Aggiornamenti dei driver di Windows", solo i driver di dispositivo vengono scaricati e archiviati nel repository. Gli aggiornamenti firmware vengono ignorati. Per informazioni sul download o l'importazione degli aggiornamenti firmware, vedere Gestione del repository degli aggiornamenti firmware.

XClarity Administrator deve essere collegato a Internet per aggiornare il catalogo e scaricare i pacchetti UXSP. Se non è collegato a Internet, è possibile scaricare manualmente il pacchetto UXSP in una workstation con accesso di rete all'host XClarity Administrator utilizzando un browser Web. Questo download UXSP è un file in formato zip e contiene tutti i file dei driver di dispositivo richiesti per il pacchetto UXSP, incluso il file di payload (.exe), i metadati (.xml), il file della cronologia delle modifiche (.chg) e i file readme (.txt).

Nota: Potrebbero essere visualizzati messaggi che indicano che i file del firmware (fw) non sono necessari e sono stati rimossi. Ciò è normale, poiché mediante questo processo vengono aggiornati solo i driver di dispositivo di Windows.



Attenzione:

- Non decomprimere il pacchetto UXSP prima di importarlo.

- I pacchetti UXSP di Windows includono i driver di dispositivo e gli aggiornamenti firmware. Gli aggiornamenti firmware nei pacchetti UXSP di Windows vengono eliminati quando i pacchetti UXSP vengono importati nel repository e viene visualizzato un messaggio di avvertenza. Solo i driver di dispositivo vengono importati.

Passo 3. **Applicazione dei driver di dispositivo del sistema operativo**

XClarity Administrator non aggiorna automaticamente i driver di dispositivo dei server gestiti. Per aggiornare i driver di dispositivo, è necessario applicare manualmente i driver di dispositivo sui server selezionati.

Attenzione: Prima di tentare di aggiornare i driver di dispositivo sui server gestiti, accertarsi di aver esaminato le seguenti considerazioni e di aver completato le azioni applicabili per i prerequisiti.

- Non è possibile selezionare i dispositivi non supportati dagli aggiornamenti.
- Leggere le considerazioni sull'aggiornamento dei driver di dispositivo, prima di tentare di aggiornare i driver di dispositivo sui server gestiti (vedere Considerazioni sull'aggiornamento dei driver di dispositivo del sistema operativo).
- Accertarsi che il repository contenga i pacchetti UXSP e i driver di dispositivo che si intende distribuire (vedere Download dei driver di dispositivo di Windows).

  Nota: Quando XClarity Administrator viene installato per la prima volta, il catalogo e il repository sono vuoti.
- XClarity Administrator può utilizzare il servizio Gestione remota Windows (WinRM) in ascolto su HTTPS o HTTP per eseguire i comandi di aggiornamento dei driver di dispositivo sui sistemi Windows di destinazione. HTTPS è l'impostazione predefinita. Per utilizzare HTTP, fare clic su **Tutte le azioni → Impostazioni globali** nella pagina "Aggiornamenti dei driver di Windows: Applica". Quindi deselezionare **Utilizza HTTPS per gli aggiornamenti dei driver di Windows**.

  Attenzione: Quando si utilizza HTTP, le credenziali utente di Windows vengono inviate in rete *senza* crittografia e possono essere visualizzate facilmente utilizzando comuni strumenti di risoluzione dei problemi.

  Importante:

  – Verificare che Gestione remota Windows (WinRM) sul server di destinazione sia configurato per utilizzare la stessa impostazione (HTTPS o HTTP) definita in XClarity Administrator (vedere Configurazione di Windows Server per gli aggiornamenti dei driver di dispositivo del sistema operativo).

  – Verificare che WinRM sia configurato con l'autenticazione di base sul server di destinazione.

  – Quando si utilizza HTTPS, verificare che WinRM sul server di destinazione sia configurato con **allowUnencrypted=false**.
- Verificare che PowerShell sia supportato sul server di destinazione.
- Verificare che il server di destinazione sia acceso prima di tentare di aggiornare i driver di dispositivo. Se il server non è acceso, selezionare il server di destinazione e fare clic su **Tutte le azioni → Azioni di alimentazione → Accendi**.
- Verificare che XClarity Administrator disponga delle informazioni necessarie per accedere al sistema operativo host (vedere Gestione dell'accesso ai sistemi operativi sui server gestiti.
- Se si desidera utilizzare un account di dominio quando si aggiornano i driver di dispositivo del sistema operativo, assicurarsi di aver creato il file di configurazione richiesto (vedere Configurazione di un account di dominio per gli aggiornamenti dei driver di dispositivo del sistema operativo).

- Verificare che nessun processo sia attualmente in esecuzione sul server di destinazione. Non è possibile aggiornare i driver di dispositivo su un server gestito bloccato da un processo in esecuzione. Se un altro processo di aggiornamento è in esecuzione sul server di destinazione, questo processo di aggiornamento viene messo in coda finché non viene completato il processo di aggiornamento corrente. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio → Processi**.

Per ulteriori informazioni sull'aggiornamento dei driver di dispositivo, vedere Applicazione dei driver di dispositivo di Windows.

Considerazioni sull'aggiornamento dei driver di dispositivo del sistema operativo

Prima di iniziare l'aggiornamento dei driver di dispositivo del sistema operativo per i dispositivi gestiti mediante Lenovo XClarity Administrator, leggere le seguenti importanti considerazioni.

Nota: È necessario disporre dell'autorità **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** o **lxc-hw-admin** per gestire e distribuire i driver di dispositivo, nonché per eseguire azioni di alimentazione sui server gestiti dalle pagine "Aggiornamenti dei driver di Windows".

Considerazioni sulla rete

- Le porte e gli indirizzi Internet richiesti devono essere disponibili, prima di tentare di scaricare i pacchetti UpdateXpress System Packs (UXSPs). Per ulteriori informazioni, vedere Disponibilità della porta e Firewall e server proxy nella documentazione online di XClarity Administrator.
- Per accedere al sistema operativo, XClarity Administrator deve disporre dell'accesso alla rete di dati e gestione.
- XClarity Administrator deve essere in grado di comunicare con il server di destinazione (sia con il controller di gestione della scheda di base sia con la rete di dati del server) sull'interfaccia di rete (Eth0 o Eth1) selezionata al momento della configurazione dell'accesso di rete di XClarity Administrator e che l'interfaccia sia configurata con un indirizzo IPv4 o ULA automatico IPv6.

  Per specificare un'interfaccia da utilizzare per la distribuzione del sistema operativo, vedere Configurazione dell'accesso alla rete).

  Per ulteriori informazioni sulla rete di distribuzione del sistema operativo e sulle interfacce, vedere Considerazioni sulla rete nella documentazione online di XClarity Administrator.
- Gli indirizzi IP devono essere univoci per il sistema operativo host.
- XClarity Administrator può utilizzare il servizio Gestione remota Windows (WinRM) in ascolto su HTTPS o HTTP per eseguire i comandi di aggiornamento dei driver di dispositivo sui sistemi Windows di destinazione. HTTPS è l'impostazione predefinita. Per utilizzare HTTP, fare clic su **Tutte le azioni → Impostazioni globali** nella pagina "Aggiornamenti dei driver di Windows: Applica". Quindi deselezionare **Utilizza HTTPS per gli aggiornamenti dei driver di Windows**.

  Attenzione: Quando si utilizza HTTP, le credenziali utente di Windows vengono inviate in rete *senza* crittografia e possono essere visualizzate facilmente utilizzando comuni strumenti di risoluzione dei problemi.

Considerazioni sui dispositivi gestiti

- L'aggiornamento dei driver di dispositivo di Windows non è supportato per i server ThinkAgile, ThinkSystem SR635 e ThinkSystemSR655.
- Sono supportati solo i server ThinkSystem, Lenovo System x e Lenovo Flex System.
- XClarity Administrator non convalida la relazione tra il controller di gestione e il sistema operativo. Il controller di gestione della scheda di base viene utilizzato per accendere o spegnere il server.

- Accertarsi che l'interfaccia LAN su USB sia abilitata. L'interfaccia LAN su USB viene utilizzata quando si aggiornano i driver di dispositivo del sistema operativo.

Considerazioni su driver di dispositivo e sistema operativo

- È possibile aggiornare i driver di dispositivo per i seguenti sistemi operativi.
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

  Nota: XClarity Administrator è stato testato solo con le versioni di Windows supportate da Microsoft al momento del rilascio della versione di XClarity Administrator.
- Gestione remota Windows (WinRM) deve essere configurato per HTTPS sul server di destinazione (vedere Configurazione di Windows Server per gli aggiornamenti dei driver di dispositivo del sistema operativo).
- PowerShell deve essere supportato sul server di destinazione.
- È necessario fornire le informazioni necessarie per accedere al sistema operativo host sul server di destinazione, come l'indirizzo IP del sistema operativo e le credenziali (vedere Gestione dell'accesso ai sistemi operativi sui server gestiti). È necessario fornire le credenziali per un account utente con autorità di amministratore.
- XClarity Administrator aggiorna solo i driver di dispositivo non conformi. I driver di dispositivo non sono conformi quando la versione sul server è precedente a quella del pacchetto UXSP selezionato. I driver di dispositivo con versione uguale o precedente a quella del pacchetto UXSP selezionato vengono ignorati.
- La conformità dei driver di dispositivo è accurata solo quando l'hardware è presente. Se l'hardware non è presente, i driver di dispositivo vengono comunque applicati al server. Quando l'hardware mancante viene aggiunto al server, Windows carica la versione più recente.
- I server System x non supportano alcuni driver di dispositivo predefiniti forniti con XClarity Administrator. Per distribuire i driver di dispositivo a questi server, creare un profilo personalizzato che includa solo i driver di dispositivo necessari.

Gestione del repository dei driver di dispositivo del sistema operativo

Il *repository dei driver di dispositivo del sistema operativo* include il catalogo e i driver di dispositivo di Windows scaricati.

Informazioni su questa attività

Il *catalogo* contiene informazioni su tutti i pacchetti UXSPs (UpdateXpress System Packs) e gli aggiornamenti dei driver di dispositivo di Windows, disponibili per tutti i server Lenovo che supportano Windows. Il catalogo organizza gli aggiornamenti dei driver di dispositivo per tipo di dispositivo. Quando si aggiorna il catalogo, XClarity Administrator recupera le informazioni sui pacchetti UXSP disponibili dal Sito Web dell'Assistenza del Centro Dati Lenovo (come i file metadata.xml e readme.txt) e memorizza le informazioni nel repository. Il file di payload (.exe) non è stato scaricato. Per ulteriori informazioni sull'aggiornamento del catalogo, vedere Aggiornamento del catalogo dei driver di dispositivo del sistema operativo.

Windows UpdateXpress System Packs (UXSPs) contiene i driver di dispositivo per le versioni supportate di Windows e per i server Lenovo che supportano Windows. È possibile scaricare o importare gli UXSPs di Windows nel repository. I pacchetti UXSPs di Windows contengono i driver di dispositivo di WIndows per le versioni supportate di Windows e per i server Lenovo che supportano Windows. I pacchetti UXSPs devono essere disponibili nel repository prima che sia possibile aggiornare i driver di dispositivo di Windows sui server gestiti.Per ulteriori informazioni sul download dei driver di dispositivo, vedere Download dei driver di dispositivo di Windows .

XClarity Administrator deve essere collegato a Internet per aggiornare il catalogo e scaricare i pacchetti UXSP. Se non è collegato a Internet, è possibile scaricare manualmente il pacchetto UXSP in una workstation con accesso di rete all'host XClarity Administrator utilizzando un browser Web. Questo download UXSP è un file in formato zip e contiene tutti i file dei driver di dispositivo richiesti per il pacchetto UXSP, incluso il file di payload (.exe), i metadati (.xml), il file della cronologia delle modifiche (.chg) e i file readme (.txt).

Una volta scaricato un pacchetto UXSP nel repository, le informazioni su ciascun driver di dispositivo nel pacchetto vengono aggiunte alla pagina "Repository degli aggiornamenti dei driver di Windows". Tra queste vi sono data di rilascio, dimensione e gravità. La gravità indica l'impatto e la necessità di applicare gli aggiornamenti utili a valutare come il proprio ambiente potrebbe essere interessato.

- **Release iniziale**. Questa è la prima versione del driver di dispositivo.
- **Critico**. Il driver di dispositivo contiene correzioni urgenti per problemi relativi al danneggiamento dei dati, alla sicurezza o alla stabilità.
- **Consigliato**. Il driver di dispositivo contiene correzioni significative per i problemi che potrebbero verificarsi.
- **Non critico**. Il driver di dispositivo contiene correzioni minori, miglioramenti delle prestazioni e modifiche testuali.

Nota:

- La gravità è relativa alla versione del driver di dispositivo rilasciata in precedenza. Ad esempio, se il driver di dispositivo è v1.01 e l'aggiornamento v1.02 è Critico mentre l'aggiornamento v1.03 è Consigliato, ciò significa che l'aggiornamento da 1.02 a 1.03 è consigliato, ma aggiornamento da v1.01 a v1.03 è critico poiché è cumulativo (v1.03 include le correzioni ai problemi critici disponibili in v1.02).
- Casi speciali potrebbero verificarsi se un aggiornamento è solo critico o consigliato per un tipo specifico di macchina. Fare riferimento alle note di rilascio per ulteriori informazioni.

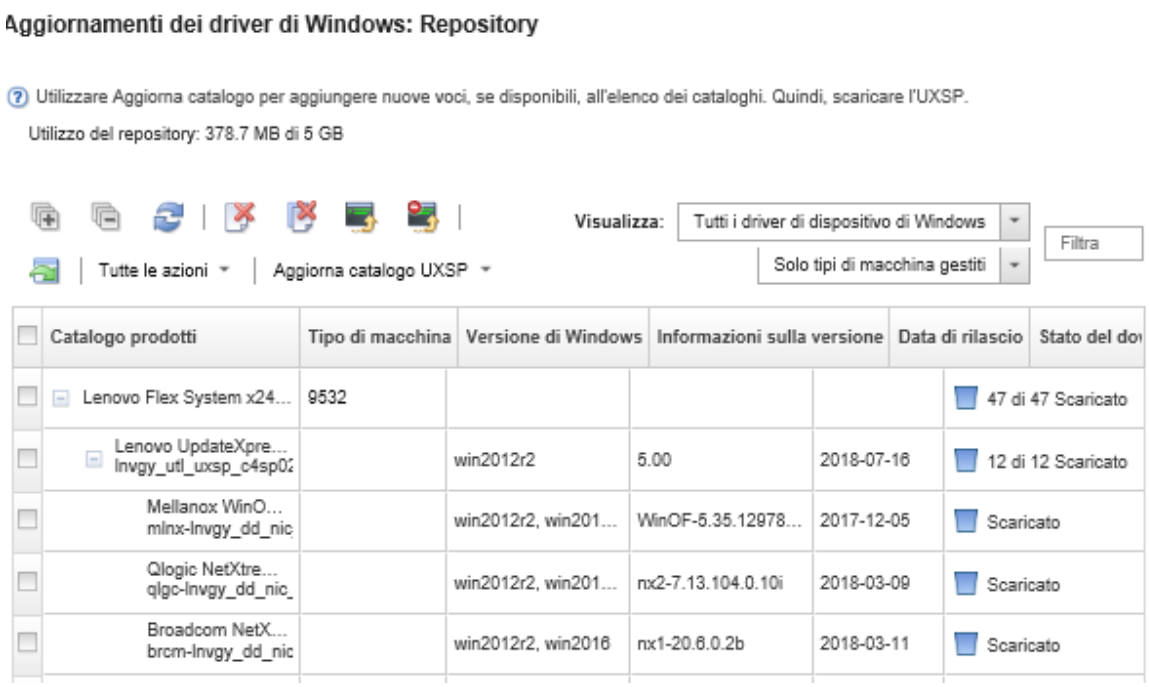
Procedura

Per visualizzare i pacchetti UXSP e i driver di dispositivo disponibili nel repository, completare le seguenti operazioni.

Passo 1. Dalla barra di menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti dei driver di Windows: repository**. Viene visualizzata la pagina Repository degli aggiornamenti dei driver di Windows con un elenco dei pacchetti UXSP disponibili, organizzati per tipo di dispositivo.

Passo 2. Espandere un tipo di server e quindi i pacchetti UXSP disponibili per quel tipo di server per visualizzare l'elenco dei driver di dispositivo disponibili per quel tipo di server.

È possibile ordinare le colonne della tabella e fare clic sull'icona **Espandi tutto** ( ) e l'icona **Comprimi tutto** ( ) per semplificare la ricerca di driver di dispositivo specifici. Inoltre, è possibile filtrare l'elenco dei tipi di server e dei driver di dispositivo visualizzati, selezionando un'opzione nel menu **Mostra** per elencare solo i driver di dispositivo di un periodo specifico, per tutti i tipi di server o solo per tipi di server gestiti. In alternativa, è possibile immettere il testo nel campo **Filtro**.



Da questa pagina, è possibile eseguire le seguenti azioni:

- Recuperare le informazioni più recenti sui pacchetti UXSP disponibili, facendo clic su **Aggiorna catalogo**.

  Il recupero di queste informazioni potrebbe richiedere alcuni minuti. Per ulteriori informazioni, vedere Aggiornamento del catalogo dei driver di dispositivo del sistema operativo.
- Scaricare i pacchetti UXSP e i driver di dispositivo mediante XClarity Administrator, aggiornando il catalogo e quindi facendo clic sull'icona **Scarica** ( ). Quando i pacchetti UXSP e i driver di dispositivo sono stati scaricati e aggiunti al repository, lo stato viene modificato in "Scaricato".

  Per ulteriori informazioni sul download dei pacchetti UXSP e dei driver di dispositivo, vedere Download dei driver di dispositivo di Windows .
- Importare i pacchetti UXSP scaricati manualmente su una workstation dal Web o i driver di dispositivo esportati da XClarity Administrator (vedere Download dei driver di dispositivo di Windows).
- Interrompere i download selezionati attualmente in corso, facendo clic sull'icona **Annulla download** ( ).
- Eliminare i pacchetti UXSP selezionati o i singoli driver di dispositivo dal repository, facendo clic sull'icona **Elimina** ( ).

Aggiornamento del catalogo dei driver di dispositivo del sistema operativo

Il catalogo dei driver di dispositivo del sistema operativo contiene informazioni su tutti i pacchetti UpdateXpress System Packs (UXSPs) e i driver di dispositivo di Windows, disponibili per tutti i server Lenovo che supportano gli aggiornamenti dei driver di dispositivo di Windows.

Prima di iniziare

Verificare che Lenovo XClarity Administrator sia connesso a Internet.

Informazioni su questa attività

Quando si aggiorna il catalogo, XClarity Administrator recupera le informazioni sui pacchetti UXSP disponibili dal Sito Web dell'Assistenza del Centro Dati Lenovo (come i file metadata.xml e readme.txt) e memorizza le informazioni nel repository. Il file di payload (.exe) non è stato scaricato. È necessario scaricare i payload dei driver di dispositivo del sistema operativo e i pacchetti UXSP desiderati, prima di aggiornare i driver di dispositivo sui server gestiti. Per ulteriori informazioni sul download dei driver di dispositivo, vedere Download dei driver di dispositivo di Windows .

Nota: Il completamento dell'aggiornamento del catalogo potrebbe richiedere diversi minuti.

Procedura

Per aggiornare il catalogo, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti dei driver di Windows: Repository** per visualizzare la pagina Repository degli aggiornamenti dei driver di Windows.

Passo 2. Fare clic su **Aggiorna catalogo**, quindi selezionare una delle seguenti opzioni per ottenere informazioni sui più recenti pacchetti UXSP disponibili.

- **Aggiorna elementi selezionati - Solo il più recente**. Recupera le informazioni sulle versioni più aggiornate dei pacchetti UXSP, disponibili solo per i server selezionati.
- **Aggiorna tutto - Solo il più recente**. Recupera le informazioni sulle versioni più aggiornate dei pacchetti UXSP per tutti i server supportati.
- **Aggiorna elementi selezionati**. Recupera le informazioni sulle versioni di tutti i pacchetti UXSP, disponibili solo per i server selezionati.
- **Aggiorna tutto**. Recupera le informazioni sulle versioni di tutti i pacchetti UXSP, disponibili solo per i server supportati.

Passo 3. Fare clic su **Aggiorna catalogo** per eseguire subito l'aggiornamento oppure fare clic su **Pianifica** per pianificare l'aggiornamento in un secondo momento.

Download dei driver di dispositivo di Windows

Windows UpdateXpress System Packs (UXSPs) contiene i driver di dispositivo per le versioni supportate di Windows e per i server Lenovo che supportano Windows. È possibile scaricare o importare gli UXSPs di Windows nel repository. I pacchetti UXSPs di Windows contengono i driver di dispositivo di WIndows per le versioni supportate di Windows e per i server Lenovo che supportano Windows. I pacchetti UXSPs devono essere disponibili nel repository prima che sia possibile aggiornare i driver di dispositivo di Windows sui server gestiti.

Prima di iniziare

Verificare che tutte le porte e gli indirizzi Internet richiesti siano disponibili, prima di tentare di scaricare UpdateXpress System Packs (UXSPs). Per ulteriori informazioni, vedere Disponibilità della porta e Firewall e server proxy nella documentazione online di XClarity Administrator.

Per scaricare UXSP mediante XClarity Administrator, verificare che XClarity Administrator sia connesso a Internet.

I browser Internet Explorer e Microsoft Edge hanno un limite di caricamento di 4 GB. Se il file da importare è maggiore di 4 GB, considerare la possibilità di utilizzare un altro browser Web (come Chrome o Firefox).

Informazioni su questa attività

XClarity Administrator deve essere collegato a Internet per aggiornare il catalogo e scaricare i pacchetti UXSP. Se XClarity Administrator non è connesso a Internet, è possibile scaricare manualmente i file in una

workstation che ha accesso alla rete dell'host XClarity Administrator mediante un browser Web e quindi importare gli aggiornamenti nel repository degli aggiornamenti firmware.

È possibile determinare se i pacchetti UXSP vengono memorizzati nel repository dalla colonna **Stato del download** nella pagina "Repository degli aggiornamenti dei driver di Windows". Questa colonna contiene i seguenti valori:

- **Scaricato**. Tutti i driver di dispositivo nel pacchetto UXSP o il singolo driver di dispositivo vengono scaricati nel repository.
- *x* **di** *y* **Scaricato**. Non tutti i driver di dispositivo nel pacchetto UXSP vengono scaricati nel repository. I numeri tra parentesi indicano il numero di driver di dispositivo disponibili e il numero di driver di dispositivo scaricati.
- **Non scaricato**. Il pacchetto UXSP o il singolo driver di dispositivo è disponibile sul sito del supporto Lenovo, ma non viene scaricato nel repository.

Un messaggio viene visualizzato sulla pagina "Repository degli aggiornamenti dei driver di Windows", quando lo spazio disponibile per UXSP e i driver di dispositivo supera il 50%. Un altro messaggio viene visualizzato sulla pagina quando il repository è pieno almeno all'85%. Per ridurre lo spazio utilizzato nel repository è possibile rimuovere i file inutilizzati, selezionando i file di destinazione e quindi facendo clic sull'icona **Elimina** ( ). Per ulteriori informazioni, vedere Gestione dello spazio su disco.

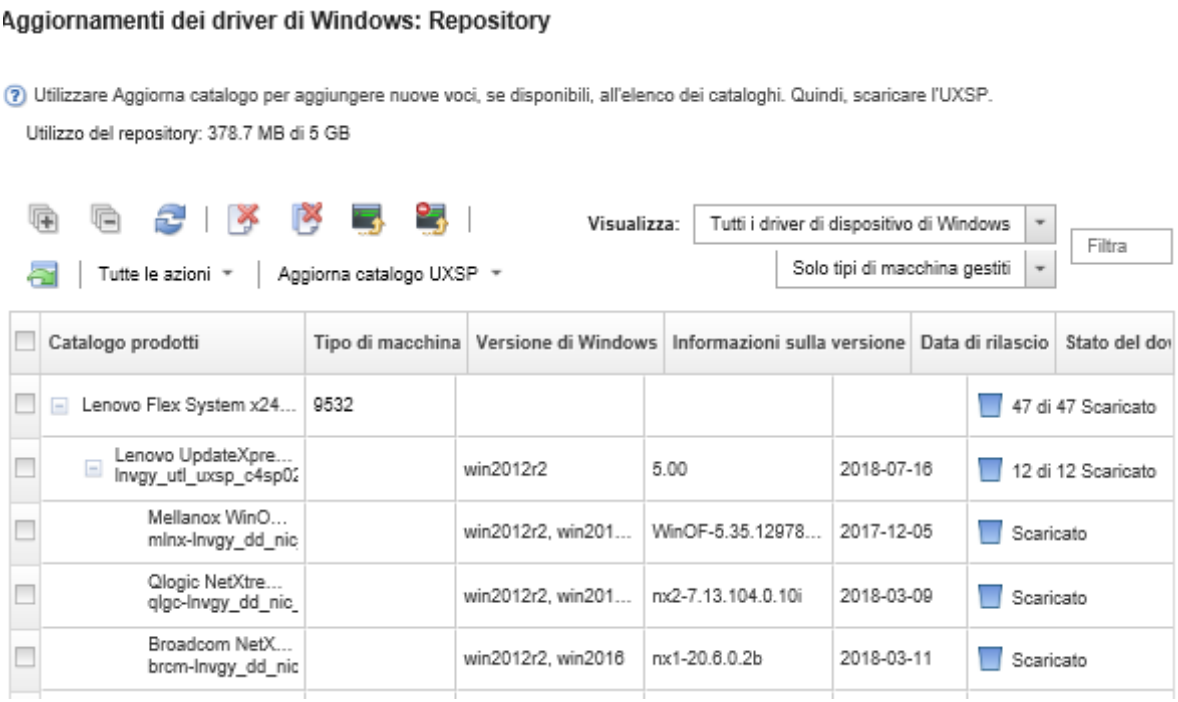
Attenzione: I pacchetti UXSP di Windows includono i driver di dispositivo e gli aggiornamenti firmware. Gli aggiornamenti firmware nei pacchetti UXSP di Windows vengono eliminati quando i pacchetti UXSP vengono importati nel repository e viene visualizzato un messaggio di avvertenza. Solo i driver di dispositivo vengono importati.

Procedura

Per scaricare i pacchetti UXSP e i driver di dispositivo specifico, effettuare una delle seguenti procedure.

- Quando XClarity Administrator è collegato a Internet:
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti dei driver di Windows: Repository** per visualizzare la pagina Repository degli aggiornamenti dei driver di Windows.
  2. Fare clic su **Aggiorna catalogo**, quindi selezionare una delle seguenti opzioni per ottenere informazioni sui più recenti pacchetti UXSP disponibili.
     - **Aggiorna elementi selezionati - Solo il più recente**. Recupera le informazioni sulle versioni più aggiornate dei pacchetti UXSP, disponibili solo per i server selezionati.
     - **Aggiorna tutto - Solo il più recente**. Recupera le informazioni sulle versioni più aggiornate dei pacchetti UXSP per tutti i server supportati.
     - **Aggiorna elementi selezionati**. Recupera le informazioni sulle versioni di tutti i pacchetti UXSP, disponibili solo per i server selezionati.
     - **Aggiorna tutto**. Recupera le informazioni sulle versioni di tutti i pacchetti UXSP, disponibili solo per i server supportati.

     Nota: Il completamento dell'aggiornamento del catalogo potrebbe richiedere diversi minuti.
  3. Espandere il tipo di server per visualizzare l'elenco dei pacchetti UXSP disponibili. Espandere il pacchetto UXSP per visualizzare un elenco dei driver di dispositivo disponibili.



4. Selezionare uno o più pacchetti UXSP di destinazione e i driver di dispositivo da scaricare.
5. Fare clic sull'icona **Scarica elementi selezionati** ( ).
6. Fare clic su **Scarica** per avviare subito il download oppure fare clic su **Pianifica** per pianificare l'esecuzione di questo download in un secondo momento.

   Il download dei pacchetti UXSP potrebbe richiedere alcuni minuti. Quando i pacchetti UXSP e i driver di dispositivo sono stati scaricati e memorizzati nel repository, la riga nel catalogo viene evidenziata e il valore della colonna **Stato del download** viene modificato in "Scaricato".

   È possibile monitorare lo stato del processo di download dal log dei processi. Dal menu XClarity Administrator, fare clic su **Monitoraggio → Processi**. Per ulteriori informazioni sul log dei processi, vedere Monitoraggio dei processi.

- Quando XClarity Administrator *non* è collegato a Internet:
  1. Scaricare i pacchetti UXSP in una workstation con connessione di rete nell'host XClarity Administrator dal Sito Web dell'Assistenza del Centro Dati Lenovo.
  2. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti dei driver di Windows: Repository** per visualizzare la pagina Repository degli aggiornamenti dei driver di Windows.
  3. Fare clic sull'icona **Importa** ( ).
  4. Fare clic su **Seleziona file** e selezionare la posizione del pacchetto UXSP sulla workstation.
  5. Selezionare il file .zip UXSP (non decomprimere il file zip prima dell'importazione), quindi fare clic su **Apri**.

     Il file .zip del pacchetto UXSP contiene il file dei metadati (.xml), il payload (.exe), il file della cronologia delle modifiche (.chg) e il file readme (.txt).
  6. Fare clic su **Importa**.

     È possibile monitorare lo stato del processo di importazione dal log dei processi. Dal menu XClarity Administrator, fare clic su **Monitoraggio → Processi**. Per ulteriori informazioni sul log dei processi, vedere Monitoraggio dei processi.

Al termine

Da questa pagina, è possibile eseguire le seguenti azioni sui pacchetti UXSP selezionati.

- Annullare un download attualmente in corso, facendo clic sull'icona **Annulla download** ().
- Eliminare tutti i file associati al pacchetto UXSP, facendo clic sull'icona **Elimina** ().

Configurazione di Windows Server per gli aggiornamenti dei driver di dispositivo del sistema operativo

Lenovo XClarity Administrator utilizza il servizio Gestione remota Windows (WinRM) in ascolto su HTTPS o HTTP per eseguire i comandi di aggiornamento dei driver di dispositivo sui sistemi Windows di destinazione. Il servizio WinRM deve essere configurato correttamente sul server di destinazione prima di tentare di aggiornare i driver di dispositivo del sistema operativo.

Prima di iniziare

Le porte richieste devono essere disponibili. Per ulteriori informazioni, vedere Disponibilità della porta nella documentazione online di XClarity Administrator.

Per ulteriori informazioni sulla configurazione di Windows Server prima di aggiornare il driver di dispositivo del sistema operativo, vedere XClarity Administrator: preparazione degli aggiornamenti dei driver di dispositivo del sistema operativo (white paper).

Procedura

Per configurare Windows Server per supportare l'aggiornamento dei driver di dispositivo del sistema operativo, completare le seguenti operazioni.

- **Per HTTPS**
  1. Firmare e installare un certificato server su ogni sistema Windows di destinazione.

     Importante: Il certificato deve contenere le seguenti informazioni.

     – Nel campo "Oggetto", verificare che sia impostato il componente di dominio (ad esempio, DC=labs, DC=com, DC=company).

     – Nel campo "Nome alternativo oggetto", verificare che siano impostati il nome DNS e l'indirizzo IP host (ad esempio, DNS Name=node1325C554A6F.labs.company.com e IP Address=10.245.43.149).
  2. Configurare i dati e i comandi di gestione remota su una connessione HTTPS eseguendo uno dei seguenti comandi da un prompt dei comandi di amministrazione. Quindi confermare le modifiche della configurazione suggerite.

     –
     ```
     winrm quickconfig -transport:https
     ```

     –
     ```
     winrm create winrm/config/Listener?Address=*+Transport=HTTPS
     @{Hostname="host_name";CertificateThumbprint="certificate_thumbprint"}
     ```

     Per configurare manualmente un listener HTTPS di WinRM secondo la documentazione WinRM, visitare la Come configurare WinRM per la pagina Web HTTPS.
  3. Abilitare l'autenticazione base degli utenti locali di Windows eseguendo il seguente comando da un prompt dei comandi di amministrazione.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```

4. Per evitare un possibile timeout e l'invio di errori di richiesta WinRM durante il controllo di conformità e l'esecuzione degli aggiornamenti dei driver, aumentare il valore predefinito per il timeout di risposta di WinRM eseguendo il comando seguente da un prompt dei comandi di amministrazione. È consigliato un valore pari a 280.000. Per ulteriori informazioni, consultare la sezione Installazione e configurazione per la pagina Web di Gestione remota Windows.
   ```
   winrm set winrm/config @{MaxTimeoutms="280000"}
   ```
5. Aprire la porta del firewall configurato per il listener HTTPS di WinRM. La porta HTTPS predefinita è 5986. Ad esempio,
   ```
   netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in action=allow
   protocol=TCP localport=5986
   ```
6. Se si utilizzano listener HTTPS, aggiungere il certificato all'archivio attendibile di XClarity Administrator, completando le seguenti operazioni. L'aggiunta del certificato all'archivio attendibile, consente a XClarity Administrator di considerare attendibili i listener HTTPS di WinRM a cui si connette. Ripetere le operazioni seguenti per i percorsi di certificazione aggiuntivi che devono essere attendibili per il servizio Gestione remota Windows.
   a. Identificare e raccogliere il certificato radice dell'autorità di certificazione utilizzato per firmare i certificati server per i sistemi Windows di destinazione. Se non si ha accesso al certificato radice CA, raccogliere il certificato server o un altro certificato nel percorso di certificazione.
   b. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Sicurezza** per visualizzare la pagina Sicurezza.
   c. Fare clic su **Certificati attendibili** nella sezione "Gestione certificati".
   d. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo Aggiungi certificato.
   e. Individuare il file del certificato raccolto nel passaggio 1 oppure copiare e incollare il contenuto del file del certificato nella casella di testo.
   f. Fare clic su **Crea**.
7. Una volta che il listener WinRM è in esecuzione sui sistemi Windows di destinazione, XClarity Administrator può connettersi a questi sistemi ed eseguire gli aggiornamenti dei driver di dispositivo.

- **Per HTTP**
  1. Configurare i dati e i comandi di gestione remota su una connessione HTTP eseguendo il seguente comando da un prompt dei comandi di amministrazione. Quindi confermare le modifiche della configurazione suggerite.
     ```
     winrm quickconfig
     ```
  2. Abilitare l'autenticazione base degli utenti locali di Windows eseguendo il seguente comando da un prompt dei comandi di amministrazione.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  3. Allocare memoria sufficiente per i comandi di aggiornamento su questo sistema eseguendo il seguente comando da un prompt dei comandi di amministrazione.
     ```
     winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
     ```
  4. Consentire i dati non crittografati eseguendo il seguente comando da un prompt dei comandi di amministrazione.
     ```
     winrm set winrm/config/service @{AllowUnencrypted="true"}
     ```
  5. Aprire la porta del firewall configurato per il listener HTTP di WinRM. La porta HTTPS predefinita è 5985. Ad esempio,
     ```
     netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-In)" dir=in action=allow
     protocol=TCP localport=5985
     ```

  Una volta che il listener WinRM è in esecuzione sui sistemi Windows di destinazione, XClarity Administrator può connettersi a questi sistemi ed eseguire gli aggiornamenti dei driver di dispositivo.

Configurazione di un account di dominio per gli aggiornamenti dei driver di dispositivo del sistema operativo

È possibile scegliere di utilizzare gli account di dominio per gestire facilmente i privilegi con un controller di dominio. Per utilizzare un account di dominio quando si aggiornano i driver di dispositivo del sistema operativo, è necessario configurare un account di dominio.

Prima di iniziare

Verificare che i server Windows gestiti si trovino in una rete di dominio prima di configurare gli account di dominio.

Quando si aggiunge l'account utente Windows in Lenovo XClarity Administrator, utilizzare il formato `USER@DOMAIN`. Il formato `DOMAIN/USER` non è supportato.

Procedura

Per configurare un account di dominio, completare la procedura che segue.

Passo 1. Dalla barra di menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Aggiornamenti dei driver di Windows: Applica**. Viene visualizzata la pagina Aggiornamenti dei driver di Windows: Applica.

Passo 2. Fare clic su **Tutte le azioni → Gestisci account dominio**. Verrà visualizzata la pagina Account di dominio.

Passo 3. Fare clic sull'icona **Crea** ( ) per aggiungere un'area di autenticazione per l'account di dominio. Verrà visualizzata la finestra di dialogo Crea area di autenticazione.

Passo 4. Specificare un nome e uno o più nomi host del centro di distribuzione delle chiavi per l'area di autenticazione. Utilizzare l'icona **Aggiungi** ( ) per aggiungere un altro nome host e l'icona **Rimuovi** ( ) per rimuovere un nome host.

Passo 5. Fare clic su **OK** per salvare l'area di autenticazione.

Passo 6. Nella pagina Account di dominio selezionare facoltativamente l'area di autenticazione da utilizzare per impostazione predefinita.

Passo 7. Fare clic su **Salva** per salvare la configurazione.

Al termine

Nella pagina di configurazione dell'account di dominio è possibile effettuare le operazioni che seguono.

- Modificare un'area di autenticazione selezionata facendo clic sull'icona **Modifica** ( ).
- Eliminare un'area di autenticazione selezionata facendo clic sull'icona **Elimina** ( ).

Configurazione delle impostazioni di aggiornamento globali dei driver di dispositivo di Windows

Le impostazioni globali fungono da impostazioni predefinite quando vengono applicati gli aggiornamenti dei driver di dispositivo di Windows.

Informazioni su questa attività

Nella pagina Impostazioni globali è possibile configurare le seguenti impostazioni:

- Utilizza HTTPS per gli aggiornamenti dei driver di Windows

- Mostra driver di dispositivo per l'hardware installato

Procedura

Per configurare le impostazioni globali da utilizzare per tutti i server, completare le seguenti operazioni.

Passo 1. Dalla barra di menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Aggiornamenti dei driver di Windows: Applica**. Viene visualizzata la pagina Aggiornamenti dei driver di Windows: Applica.

Passo 2. Fare clic su **Tutte le azioni → Impostazioni globali** per visualizzare la finestra di dialogo Impostazioni globali: applica aggiornamenti dei driver di Windows.

Passo 3. Facoltativamente, selezionare una delle seguenti opzioni:

- Selezionare **Utilizza HTTPS per gli aggiornamenti dei driver di Windows** per utilizzare il servizio Gestione remota Windows (WinRM) in ascolto su HTTPS per eseguire i comandi di aggiornamento dei driver di dispositivo sui sistemi Windows di destinazione. HTTPS è l'impostazione predefinita.

  Deselezionare questa impostazione per utilizzare HTTP.

  Attenzione: Quando si utilizza HTTP, le credenziali utente di Windows vengono inviate in rete *senza* crittografia e possono essere visualizzate facilmente utilizzando comuni strumenti di risoluzione dei problemi.
- Selezionare **Mostra driver di dispositivo per l'hardware installato** per visualizzare un elenco dei soli driver di dispositivo per l'hardware gestito.

  Deselezionare questa impostazione per visualizzare l'elenco di tutti i driver di dispositivo di ciascun pacchetto UpdateXpress System Packs (UXSPs) importato.

  Importante: una volta selezionata questa opzione, è necessario eseguire un controllo di conformità facendo clic sull'icona **Controlla conformità** ( ) nella pagina Aggiornamenti dei driver di Windows: Applica.

Passo 4. Fare clic su **OK** per chiudere la finestra di dialogo.

Applicazione dei driver di dispositivo di Windows

È possibile applicare i driver di dispositivo ai server gestiti con Windows.

Prima di iniziare

- Lenovo XClarity Administrator utilizza il servizio Gestione remota Windows (WinRM) in ascolto su HTTPS o HTTP per eseguire i comandi di aggiornamento dei driver di dispositivo sui sistemi Windows di destinazione. Il servizio WinRM deve essere configurato correttamente sul server di destinazione prima di

tentare di aggiornare i driver di dispositivo del sistema operativo (vedere Configurazione di Windows Server per gli aggiornamenti dei driver di dispositivo del sistema operativo).

- Non è possibile selezionare i dispositivi non supportati dagli aggiornamenti.
- Leggere le considerazioni sull'aggiornamento dei driver di dispositivo, prima di tentare di aggiornare i driver di dispositivo sui server gestiti (vedere Considerazioni sull'aggiornamento dei driver di dispositivo del sistema operativo).
- Accertarsi che il repository contenga i pacchetti UXSP e i driver di dispositivo che si intende distribuire (vedere Download dei driver di dispositivo di Windows).

  Nota: Quando XClarity Administrator viene installato per la prima volta, il catalogo e il repository sono vuoti.
- XClarity Administrator può utilizzare il servizio Gestione remota Windows (WinRM) in ascolto su HTTPS o HTTP per eseguire i comandi di aggiornamento dei driver di dispositivo sui sistemi Windows di destinazione. HTTPS è l'impostazione predefinita. Per utilizzare HTTP, fare clic su **Tutte le azioni → Impostazioni globali** nella pagina "Aggiornamenti dei driver di Windows: Applica". Quindi deselezionare **Utilizza HTTPS per gli aggiornamenti dei driver di Windows**.

  Attenzione: Quando si utilizza HTTP, le credenziali utente di Windows vengono inviate in rete *senza* crittografia e possono essere visualizzate facilmente utilizzando comuni strumenti di risoluzione dei problemi.

  Importante:

  – Verificare che Gestione remota Windows (WinRM) sul server di destinazione sia configurato per utilizzare la stessa impostazione (HTTPS o HTTP) definita in XClarity Administrator (vedere Configurazione di Windows Server per gli aggiornamenti dei driver di dispositivo del sistema operativo).

  – Verificare che WinRM sia configurato con l'autenticazione di base sul server di destinazione.

  – Quando si utilizza HTTPS, verificare che WinRM sul server di destinazione sia configurato con **allowUnencrypted=false**.
- Verificare che PowerShell sia supportato sul server di destinazione.
- Verificare che il server di destinazione sia acceso prima di tentare di aggiornare i driver di dispositivo. Se il server non è acceso, selezionare il server di destinazione e fare clic su **Tutte le azioni → Azioni di alimentazione → Accendi**.
- Verificare che XClarity Administrator disponga delle informazioni necessarie per accedere al sistema operativo host (vedere Gestione dell'accesso ai sistemi operativi sui server gestiti.
- Se si desidera utilizzare un account di dominio quando si aggiornano i driver di dispositivo del sistema operativo, assicurarsi di aver creato il file di configurazione richiesto (vedere Configurazione di un account di dominio per gli aggiornamenti dei driver di dispositivo del sistema operativo).
- Verificare che nessun processo sia attualmente in esecuzione sul server di destinazione. Non è possibile aggiornare i driver di dispositivo su un server gestito bloccato da un processo in esecuzione. Se un altro processo di aggiornamento è in esecuzione sul server di destinazione, questo processo di aggiornamento viene messo in coda finché non viene completato il processo di aggiornamento corrente. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio → Processi**.

Informazioni su questa attività

XClarity Administrator aggiorna solo i driver di dispositivo non conformi. I driver di dispositivo non sono conformi quando la versione sul server è precedente a quella del pacchetto UXSP selezionato. I driver di dispositivo con versione uguale o precedente a quella del pacchetto UXSP selezionato vengono ignorati.

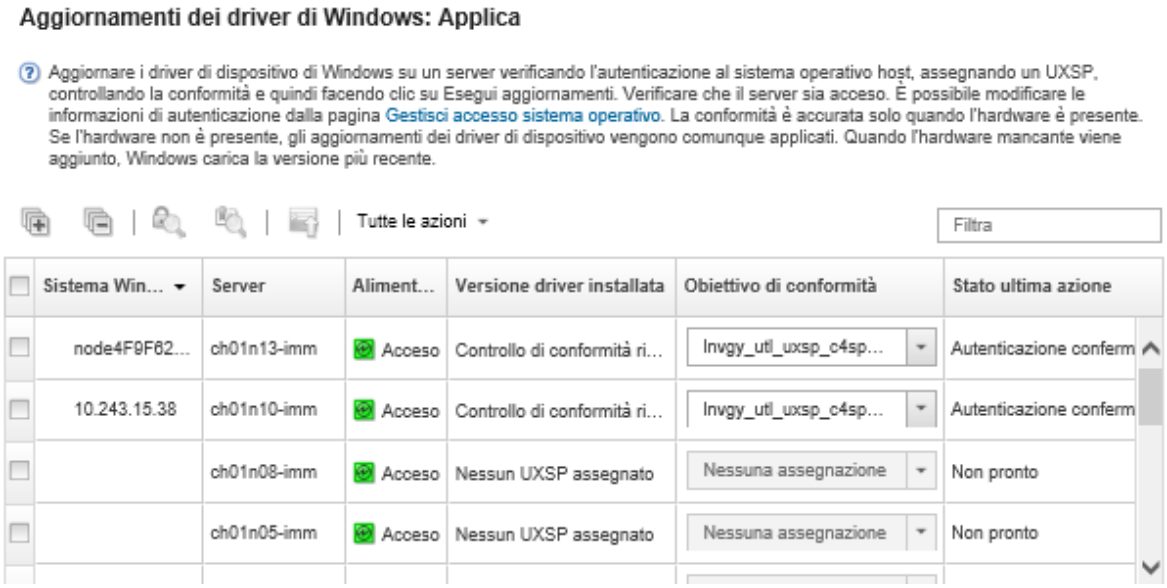
Procedura

Per applicare i driver di dispositivo di Windows ai server gestiti, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Aggiornamenti dei driver di Windows: Applica** per visualizzare la pagina Aggiornamenti dei driver di Windows: Applica.

Importante:

- Per rilevare i driver di dispositivo sul server di destinazione e determinare la conformità, è necessario selezionare il server di destinazione ed eseguire il controllo di conformità. Una volta eseguito il controllo di conformità per la prima volta, è possibile espandere la riga per visualizzare un elenco dei driver di dispositivo sul server di destinazione.
- La colonna **Sistema Windows** identifica il nome host o l'indirizzo IP del sistema operativo host.
- La colonna **Server** identifica il nome e l'indirizzo IP del server gestito.



Passo 2. Selezionare uno o più server di destinazione e i driver di dispositivo.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. È inoltre possibile filtrare l'elenco dei server visualizzati, immettendo il testo (come, il nome o l'indirizzo IP) nel campo **Filtro**.

Suggerimento:

- È possibile scegliere di aggiornare tutti i driver di dispositivo per un sistema operativo specifico oppure di espandere un sistema operativo e scegliere di aggiornare solo specifici dispositivi
- La colonna **Stato aggiornamento** mostra lo stato di autenticazione per ciascun server e lo stato di aggiornamento per ogni driver di dispositivo.
- La colonna **Credenziali sistema operativo** mostra le credenziali memorizzate, utilizzate per eseguire l'autenticazione al sistema operativo (ad esempio, "901 – company\USER1").

  Se le credenziali del sistema operativo non sono definite per il sistema operativo host sul server di destinazione, viene visualizzata la finestra di dialogo Modifica credenziali sistema operativo. Per un singolo server di destinazione, specificare il nome utente e la password che si desidera utilizzare per questa operazione. Per più server di destinazione, selezionare la credenziale memorizzata da utilizzare per ciascun server. Quindi, fare clic su **Salva**.

Nota: Le credenziali del sistema operativo selezionate nella finestra di dialogo Modifica credenziali sistema operativo non vengono salvate per il sistema operativo host. Per salvare le credenziali del sistema operativo, vedere Gestione dell'accesso ai sistemi operativi sui server gestiti.

Passo 3. Fare clic sull'icona **Controlla autenticazione** () per eseguire i controlli di autenticazione e dei prerequisiti.

XClarity Administrator si collega al sistema operativo host utilizzando le credenziali memorizzata riportate nella colonna **Credenziali sistema operativo**, determina la versione del sistema operativo, verifica che WinRM sia abilitato, esegue ulteriori controlli dei prerequisiti e quindi si disconnette dal sistema operativo dell'host.

Per informazioni su come modificare le credenziali memorizzate per il sistema operativo host, vedere Gestione dell'accesso ai sistemi operativi sui server gestiti.

Passo 4. Per ciascun server di destinazione, selezionare il pacchetto UXSP di destinazione che si desidera utilizzare per aggiornare i driver di dispositivo dalla colonna **Obiettivo di conformità**.

Passo 5. Selezionare nuovamente il server di destinazione e fare clic sull'icona **Controlla conformità** () per verificare la conformità di ogni driver di dispositivo.

Il controllo di conformità aggiorna lo stato della conformità nella colonna **Versione installata del driver**. Questa colonna consente di visualizzare lo stato globale della conformità per il server, nonché la versione installata e lo stato della conformità per ogni driver di dispositivo rispetto al pacchetto UXSP assegnato.

- **Conforme**. La versione del driver di dispositivo installato è identica o successiva a quella del pacchetto UXSP assegnato.
- **Non conforme**. La versione del driver di dispositivo installato è precedente a quella del pacchetto UXSP assegnato. È possibile fare clic sul collegamento per ottenere ulteriori informazioni sulla mancata conformità.

Nota: La conformità dei driver di dispositivo è accurata solo quando l'hardware è presente. Se l'hardware non è presente, i driver di dispositivo vengono comunque applicati al server. Quando l'hardware mancante viene aggiunto al server, Windows carica la versione più recente.

Passo 6. Fare clic sull'icona **Esegui aggiornamenti** ().

Passo 7. Selezionare una delle seguenti regole di aggiornamento.

- **Interrompi tutti gli aggiornamenti in caso di errore**. Se si verifica un errore durante l'aggiornamento dei driver di dispositivo su un dispositivo di destinazione, il processo di aggiornamento viene interrotto per tutti i dispositivi di destinazione nel processo di aggiornamento corrente dei driver di dispositivo. In questo caso, non viene applicato alcun aggiornamento dei driver di dispositivo nel pacchetto UXSP per il dispositivo di destinazione. Il driver di dispositivo corrente installato su tutti i dispositivi di destinazione rimane valido.
- **Continua in caso di errore**. Se si verifica un errore durante l'aggiornamento dei driver di dispositivo sul dispositivo di destinazione, il processo di aggiornamento non aggiorna il driver di dispositivo per quel dispositivo specifico; tuttavia, il processo di aggiornamento continua ad aggiornare gli altri driver di dispositivo sul dispositivo e tutti gli altri dispositivi di destinazione nel processo di aggiornamento del driver di dispositivo corrente.
- **Continuare con il sistema successivo durante un errore**. Se si verifica un errore durante l'aggiornamento dei driver di dispositivo, il processo di aggiornamento interrompe ogni tentativo di aggiornare i driver di dispositivo per quel dispositivo specifico, in modo che i driver di dispositivo correntemente installati restino validi. Il processo di aggiornamento continua ad

aggiornare tutti gli altri dispositivi nel processo corrente di aggiornamento dei driver di dispositivo.

Passo 8. Fare clic su **Esegui aggiornamenti** per eseguire subito l'aggiornamento oppure fare clic su **Pianifica** per pianificare l'esecuzione di questo aggiornamento in un secondo momento.

Al termine

Quando si applica un aggiornamento, se il server di destinazione non entra in modalità di manutenzione, tentare di applicare nuovamente l'aggiornamento.

Se gli aggiornamenti non sono stati completati correttamente, vedere Considerazioni sull'aggiornamento dei driver di dispositivo del sistema operativo per la risoluzione dei problemi e le azioni correttive.

Dalla pagina Aggiornamenti dei driver di Windows: Applica è possibile eseguire le seguenti azioni.

- Visualizzare lo stato dell'aggiornamento dei driver di dispositivo direttamente dalla pagina "Applica" nella colonna **Stato aggiornamento**.
- Monitorare lo stato dell'aggiornamento dei driver di dispositivo dal log dei processi. Dal menu XClarity Administrator, fare clic su **Monitoraggio → Processi**.

  Per ulteriori informazioni sul log dei processi, vedere Monitoraggio dei processi.

  Una volta completato il processo di aggiornamento, è possibile verificare che i dispositivi siano conformi dalla pagina "Aggiornamenti dei driver di Windows: Applica". La versione corrente del driver attiva su ciascun dispositivo è riportata nella colonna **Versione installata del driver**.

Capitolo 15. Installazione dei sistemi operativi sui server bare metal

È possibile utilizzare Lenovo XClarity Administrator per gestire il repository di immagini del sistema operativo e distribuire le immagini del sistema operativo fino a 28 server bare-metal contemporaneamente.

Ulteriori informazioni:

- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: distribuzione del sistema operativo

Prima di iniziare

Al termine del periodo di prova di 90 giorni, è possibile continuare a utilizzare XClarity Administrator per gestire e monitorare l'hardware gratuitamente; tuttavia, è necessario acquistare le licenze per l'attivazione di tutte le funzioni per ciascun server gestito che supporta le funzioni avanzate di XClarity Administrator per continuare a utilizzare la funzione di distribuzione del sistema operativo. Lenovo XClarity Pro dà diritto a usufruire del servizio di assistenza e supporto e a utilizzare la licenza per l'attivazione di tutte le funzioni. Per ulteriori informazioni sull'acquisto di Lenovo XClarity Pro, contattare un rappresentante Lenovo o un business partner autorizzato. Per ulteriori informazioni, vedere Installazione della licenza di abilitazione di tutte le funzionalità nella documentazione online di XClarity Administrator.

Informazioni su questa attività

XClarity Administrator fornisce un modo semplice per distribuire le immagini del sistema operativo sui server *bare metal*, su cui generalmente non è installato un sistema operativo.

Attenzione: Se si distribuisce un sistema operativo su un server su cui è installato un sistema operativo, XClarity Administrator esegue una nuova installazione che sovrascrive le partizioni sui dischi di destinazione

La quantità di tempo necessaria per distribuire un sistema operativo su un server è determinata da vari fattori:

- La quantità di RAM installata nel server, che incide sul tempo che il server impiega per l'avvio.
- Il numero e i tipi di adattatori I/O installati nel server, che incide sulla quantità di tempo che XClarity Administrator impiega per eseguire un inventario del server. Incide, inoltre, sulla quantità di tempo necessaria per l'avvio del firmware UEFI quando il server viene avviato. Durante una distribuzione del sistema operativo, il server viene riavviato più volte.
- Traffico di rete. XClarity Administrator scarica l'immagine del sistema operativo sulla rete di dati o sulla rete di distribuzione del sistema operativo.
- La configurazione hardware sull'host su cui è installata l'appliance virtuale Lenovo XClarity Administrator. La quantità di RAM, di processori e di storage dell'unità disco fisso che possono incidere sui tempi del download.

Importante: Per distribuire un'immagine del sistema operativo da XClarity Administrator, almeno una delle interfacce (Eth0 o Eth1) di XClarity Administrator deve disporre della connettività di rete IP sull'interfaccia di rete del server che viene utilizzata per accedere al sistema operativo host. La distribuzione del sistema operativo utilizza l'interfaccia definita nella pagina Accesso alla rete. Per ulteriori informazioni sulle impostazioni di rete, vedere Configurazione dell'accesso alla rete.

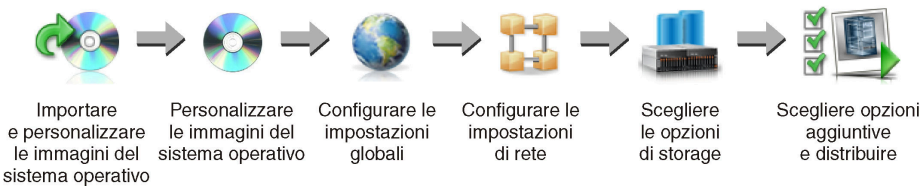
Prima di eseguire una distribuzione del sistema operativo bare metal su un server, preparare il server aggiornando il firmware ai livelli più recenti e configurare il server utilizzando i Pattern di configurazione. Per

ulteriori informazioni, vedere Aggiornamento del firmware sui dispositivi gestiti, Configurazione dei server mediante i pattern di configurazione.

Attenzione: si consiglia di *non* utilizzare XClarity Administrator per eseguire una distribuzione del sistema operativo bare metal sulle appliance Converged e ThinkAgile.

Procedura

La seguente figura mostra il flusso di lavoro per la distribuzione di un'immagine del sistema operativo su un server.



Passo 1. **Importare le immagini del sistema operativo.**

Prima di poter distribuire un'immagine del sistema operativo su un server, è necessario prima importare il sistema operativo nel repository. Quando si importa un'immagine del sistema operativo, XClarity Administrator:

- Verifica che ci sia spazio sufficiente nel repository di immagini del sistema operativo prima di importare il sistema operativo. Se non si dispone di spazio sufficiente per l'importazione di un'immagine, eliminare un'immagine esistente dal repository e tentare di importare nuovamente la nuova immagine.
- Crea uno o più profili dell'immagine e memorizza il profilo nel repository di immagini del sistema operativo. Ciascun *profilo* include l'immagine del sistema operativo e le opzioni di installazione. Per ulteriori informazioni sui profili predefiniti dell'immagine del sistema operativo, vedere Profili immagine del sistema operativo.

Un *sistema operativo di base* è l'immagine completa del sistema operativo importata nel repository di immagini del sistema operativo. L'immagine di base importata contiene i profili predefiniti che descrivono le configurazioni di installazione per l'immagine. È possibile creare profili personalizzati nell'immagine del sistema operativo di base, che possono essere distribuiti per configurazioni specifiche.

È inoltre possibile importare *sistemi operativi personalizzati* supportati. Questa immagine personalizzata contiene un profilo segnaposto predefinito, che non può essere distribuito. È necessario importare un profilo personalizzato che può essere distribuito o creare un proprio profilo personalizzato basato sul profilo segnaposto. Una volta aggiunto il profilo personalizzato, il profilo segnaposto viene rimosso automaticamente.

Per Microsoft Windows Server 2016 e 2019, è possibile importare un'immagine del sistema operativo personalizzata per ogni versione. L'immagine di base importata contiene i profili predefiniti che descrivono le configurazioni di installazione per l'immagine. Non è possibile creare profili personalizzati nell'immagine del sistema operativo personalizzata.

Per un elenco dei sistemi operativi di base e personalizzati supportati, vedere Sistemi operativi supportatiSistemi operativi supportati nella documentazione online di Lenovo XClarity Administrator.

Passo 2. **(Facoltativo) Personalizzare le immagini del sistema operativo.**

È possibile personalizzare un'immagine del sistema operativo aggiungendo i driver di dispositivo, i file di avvio (solo per Windows), le impostazioni di configurazione, i file di installazione automatica, gli script post-installazione e il software. Quando si personalizza un'immagine del sistema operativo di base, XClarity Administrator crea un profilo dell'immagine del sistema operativo personalizzato che include le opzioni di installazione e i file personalizzati.

Il repository di immagini del sistema operativo consente di memorizzare un numero illimitato di file predefiniti e personalizzati, se è disponibile lo spazio per l'archiviazione dei file.

Passo 3. **Configurare le impostazioni globali.**

Le impostazioni globali sono opzioni di configurazione che fungono da impostazioni predefinite per la distribuzione del sistema operativo. È possibile configurare le seguenti impostazioni globali.

- La password per l'account utente dell'amministratore da utilizzare per distribuire i sistemi operativi
- Il metodo da utilizzare per assegnare gli indirizzi IP ai server
- I codici di licenza da utilizzare quando si attivano i sistemi operativi installati
- Facoltativamente, unire un dominio di Active Directory nell'ambito della distribuzione del sistema operativo Windows

Passo 4. **Configurare le impostazioni di rete.**

È possibile specificare le impostazioni di rete per ciascun server su cui i sistemi operativi devono essere distribuiti.

Se si utilizza DHCP per assegnare dinamicamente gli indirizzi IP, è necessario configurare l'indirizzo MAC.

Se si utilizzano indirizzi IP statici, è necessario configurare le seguenti impostazioni di rete per un server specifico prima di poter distribuire un sistema operativo a tale server. Dopo aver configurato tali impostazioni, lo stato di distribuzione delle modifiche del server viene modificato in "Pronto". Alcuni campi non sono disponibili per gli indirizzi IPv6 statici.

- Nome host

  Il nome host deve essere conforme alle seguenti regole:
  - Il nome host di ciascun server gestito deve essere univoco.
  - Il nome host può contenere stringhe (etichette) separate da un punto (.).
  - Ogni etichetta può contenere lettere, numeri e trattini (-) ASCII; tuttavia, la stringa non può iniziare o terminare con un trattino e non può contenere solo numeri.
  - La prima etichetta può avere una lunghezza compresa tra 2 e 15 caratteri. Le etichette successive possono avere una lunghezza compresa tra 2 e 63 caratteri.
  - La lunghezza totale del nome host non deve superare i 255 caratteri.
- L'indirizzo MAC della porta sull'host in cui deve essere installato il sistema operativo.

  L'indirizzo MAC è impostato su AUTO per impostazione predefinita. Questa impostazione rileva automaticamente le porte Ethernet che possono essere configurate e utilizzate per la distribuzione. Il primo indirizzo MAC (porta) rilevato viene utilizzato per impostazione predefinita. Se viene rilevata la connettività su un indirizzo MAC differente, l'host XClarity Administrator viene riavviato automaticamente per utilizzare l'indirizzo MAC appena rilevato per la distribuzione.

  È possibile determinare lo stato della porta dell'indirizzo MAC utilizzata per la distribuzione del sistema operativo dal menu a discesa **Indirizzo MAC** nella finestra di dialogo Impostazioni di rete. Se sono presenti più porte o se tutte le porte sono disattivate, viene utilizzato AUTO per impostazione predefinita.

Nota:

- Le porte di rete virtuali non sono supportate. Non utilizzare una porta di rete fisica per simulare più porte di rete virtuali.
- Quando l'impostazione di rete del server è configurata su AUTO, XClarity Administrator può rilevare automaticamente le porte di rete negli slot 1-16. Almeno una porta negli slot 1-16 deve disporre di una connessione a XClarity Administrator.
- Se si desidera utilizzare una porta di rete nello slot 17 o superiore per l'indirizzo MAC, non è possibile utilizzare l'opzione AUTO. È necessario invece configurare l'impostazione di rete del server con l'indirizzo MAC della porta specifica che si desidera utilizzare.
- Per i server ThinkServer, non tutti gli indirizzi MAC host sono visualizzati. In molti casi, gli indirizzi MAC per gli adattatori Ethernet AnyFabric sono elencati nella finestra di dialogo Modifica impostazioni di rete. Gli indirizzi MAC per gli altri adattatori Ethernet (ad es. Lan-On-Motherboard) non sono elencati. Nei casi in cui l'indirizzo MAC per un adattatore non è disponibile, utilizzare il metodo AUTO per le distribuzioni non VLAN.

- Indirizzo IP e maschera di sottorete
- Gateway IP
- Fino a due server DNS (Domain Name System)
- Velocità MTU (Maximum Transmission Unit)
- ID VLAN, se la modalità IP VLAN è abilitata

Se si decide di utilizzare VLAN, è possibile assegnare un ID VLAN alla scheda di rete host configurata.

Passo 5. **Scegliere le opzioni di storage**

Per ciascuna distribuzione, è possibile scegliere la posizione di storage preferita in cui si desidera distribuire il sistema operativo. A seconda del sistema operativo, è possibile scegliere di eseguire la distribuzione su un'unità disco locale, su una chiave dell'hypervisor incorporato o su una rete SAN.

Passo 6. **Scegliere le opzioni aggiuntive e le impostazioni di configurazione personalizzate, quindi distribuire l'immagine del sistema operativo.**

È possibile configurare opzioni di distribuzione aggiuntive, ad esempio la chiave di licenza per la distribuzione del sistema operativo e le impostazioni di configurazione personalizzate. Se si installa Microsoft Windows, è possibile anche configurare il dominio di Active Directory per l'aggiunta.

Nota:

- Se sono state definite impostazioni di configurazione personalizzate per un profilo del sistema operativo personalizzato specifico, è necessario definire i valori per le impostazioni di configurazione personalizzate, prima di poter distribuire il profilo a un server.
- Durante la distribuzione di un profilo del sistema operativo personalizzato che include le impostazioni personalizzate, tutti i server di destinazione devono utilizzare lo stesso profilo del sistema operativo personalizzato e i valori per le impostazioni personalizzate si applicano a tutti i server di destinazione.

È possibile scegliere i server di destinazione per la distribuzione e le immagini del sistema operativo da distribuire. Ricordare che per distribuire un sistema operativo, lo stato di distribuzione del server deve essere "Pronto."

È possibile distribuire le immagini del sistema operativo simultaneamente su un massimo di 28 server.

Prima di tentare la distribuzione di un'immagine del sistema operativo, ricontrollare Considerazioni sulla distribuzione del sistema operativo.

Considerazioni sulla distribuzione del sistema operativo

Prima di tentare la distribuzione di un'immagine del sistema operativo, esaminare le seguenti considerazioni.

Lenovo XClarity Administrator considerazioni

- Verificare che nessun processo sia attualmente in esecuzione sul server di destinazione. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio → Processi**.
- Verificare che il server di destinazione non abbia un pattern server rinviato o parziale attivato. Se un pattern server è stato rinviato o parzialmente attivato sul server gestito, è necessario riavviare il server per applicare tutte le impostazioni di configurazione. Non tentare di distribuzione un sistema operativo su un server con un pattern server parzialmente attivato. Per determinare lo stato di configurazione del server, consultare il campo **Stato configurazione** nella pagina Riepilogo del server gestito (vedere Visualizzazione dei dettagli di un server gestito).
- Verificare che sia stata specificata una password per l'account dell'amministratore utilizzata per distribuire il sistema operativo nella finestra di dialogo Impostazioni globali: distribuisci sistemi operativi. Per ulteriori informazioni sull'impostazione della password, vedere Configurazione delle impostazioni globali di distribuzione del sistema operativo.
- Verificare che le impostazioni globali predefinite siano corrette per questa distribuzione del sistema operativo (vedere Configurazione delle impostazioni globali di distribuzione del sistema operativo).

Considerazioni sul sistema operativo

- Verificare di possedere tutte le licenze del sistema operativo applicabili per attivare i sistemi operativi installati. L'utente sarà responsabile dell'acquisizione delle licenze direttamente dal produttore del sistema operativo.
- Verificare che l'immagine del sistema operativo che si intende distribuire sia già caricata nel repository di immagini del sistema operativo. Per informazioni sull'importazione delle immagini, vedere Importazione delle immagini del sistema operativo.
- Le immagini del sistema operativo nel repository di XClarity Administrator potrebbero non essere supportate solo su determinate piattaforme hardware. Solo i profili immagine del sistema operativo supportati dal server selezionato sono elencati nella pagina "Distribuisci immagini sistema operativo". È possibile determinare se un sistema operativo è compatibile con un server specifico da Sito Web della guida all'interoperabilità del sistema operativo Lenovo.
- Per Windows, prima di poter distribuire un profilo Windows, è necessario importare un file di avvio nel repository di immagini del sistema operativo. Lenovo fornisce un bundle che include il file di avvio WinPE_64.wim predefinito e un set di driver di dispositivo in un unico pacchetto che può essere scaricato da Pagina Web dei driver di Windows Lenovo e del repository delle immagini WinPE e quindi importato nel repository delle immagini del sistema operativo. Poiché il file del bundle contiene sia i driver di dispositivo sia i file di avvio, è possibile importare il file del bundle dalla scheda **Driver di dispositivo** o **File di avvio**.
- Per SLES 15 e 15 SP1, è necessario importare sia l'immagine del programma di installazione sia l'immagine del pacchetto associato dal Pagina Web del centro di supporto del sistema operativo del server. Per SLES 15 SP2 o versione successiva, è necessario importare solo l'immagine del supporto di installazione completa, poiché i DVD dei pacchetti e del programma di installazione unificato di SUSE Linux Enterprise Server 15 e 15 SP1 sono deprecati.
- Per i server ThinkSystem, XClarity Administrator comprende i driver di dispositivo non inclusi per abilitare l'installazione del sistema operativo, nonché la configurazione base di rete e di storage per il sistema operativo finale. Per gli altri server, verificare che l'immagine del sistema operativo che si intende distribuire includa i driver di dispositivo dell'adattatore di storage, Fibre Channel ed Ethernet corretti per l'hardware. Se il driver di dispositivo dell'adattatore I/O non è incluso nel sistema operativo, l'adattatore

non è supportato per la distribuzione del sistema operativo. Installare sempre il sistema operativo più recente per accertarsi di possedere i driver di dispositivo dell'adattatore I/O integrati più recenti e i file di avvio necessari. È inoltre possibile aggiungere file di avvio e driver di dispositivo non inclusi ai sistemi operativi importati in XClarity Administrator (vedere Personalizzazione dei profili delle immagini del sistema operativo nella documentazione online di XClarity Administrator).

Per VMware, utilizzare l'immagine personalizzata Lenovo per ESXi più aggiornata, che include il supporto per gli adattatori più recenti. Per informazioni su come ottenere questa immagine, consultare il Supporto VMware - Pagina Web dei download.

- Per i server ThinkSystem, se si intende distribuire SLES 12 SP2, è necessario utilizzare un profilo kISO. Per ottenere i profili kISO, è necessario importare l'immagine kISO SLES appropriata dopo aver importato il sistema operativo SLES base. È possibile scaricare l'immagine kISO SLES da Supporto Linux - Pagina Web dei download.

  Nota:

  – L'immagine kISO SLES viene conteggiata per il numero massimo di immagini del sistema operativo importate.

    Per un elenco dei sistemi operativi di base e personalizzati supportati, vedere Sistemi operativi supportatiSistemi operativi supportati nella documentazione online di Lenovo XClarity Administrator.

  – Se si eliminano tutti i profili kISO, è necessario eliminare il sistema operativo SLES di base e quindi importare nuovamente l'immagine del sistema operativo di base e l'immagine kISO per distribuire SLES 12 SP2 su un server ThinkSystem.

  – Se si crea un profilo di sistema operativo personalizzato basato su un profilo kISO, i driver di dispositivo predefiniti del sistema operativo di base non sono inclusi. Vengono utilizzati i driver di dispositivo inclusi nel profilo kISO. È anche possibile aggiungere i driver di dispositivo al profilo del sistema operativo personalizzato (vedere Creazione di un profilo immagine del sistema operativo personalizzato).

Per ulteriori informazioni sulle limitazioni di sistemi operativi specifici, vedere Sistemi operativi supportati.

Considerazioni sulla rete

- Verificare che tutte le porte richieste siano aperte (vedere Disponibilità della porta per i sistemi operativi distribuiti).
- Verificare che XClarity Administrator possa comunicare con il server di destinazione (sia con il controller di gestione della scheda di base sia con la rete di dati dei server) sull'interfaccia (Eth0 o Eth1) selezionata al momento della configurazione dell'accesso di rete di XClarity Administrator.

  Per specificare un'interfaccia da utilizzare per la distribuzione del sistema operativo, vedere Configurazione dell'accesso alla rete).

  Per ulteriori informazioni sulla rete di distribuzione del sistema operativo e sulle interfacce, vedere Considerazioni sulla rete nella documentazione online di XClarity Administrator.
- Verificare che gli indirizzi IP siano univoci per il sistema operativo host. XClarity Administrator controlla gli indirizzi IP duplicati specificati per l'indirizzo di rete durante il processo di distribuzione.
- Se la rete è lenta o instabile, è possibile visualizzare i risultati imprevedibili durante la distribuzione dei sistemi operativi.
- Per collegare il controller di gestione della scheda di base è necessario configurare l'interfaccia di rete di XClarity Administrator utilizzata per la gestione, utilizzando lo stesso metodo dell'indirizzo IP selezionato nella finestra di dialogo Impostazioni globali: Distribuisci sistemi operativi. Ad esempio, se XClarity Administrator è configurato per utilizzare eth0 per la gestione e si sceglie di usare gli indirizzi IPv6 statici assegnati manualmente durante la configurazione del sistema operativo distribuito, eth0 deve essere configurato con un indirizzo IPv6 che disponga della connettività al controller di gestione della scheda di base.

- Se si sceglie di utilizzare gli indirizzi IPv6 per le impostazioni globali di distribuzione del sistema operativo, l'indirizzo IPv6 di XClarity Administrator deve essere instradabile al controller di gestione della scheda di base e alla rete di dati dei server.
- La modalità IPv6 non è supportata per ThinkServer (vedere Limitazioni della configurazione IPv6 nella documentazione online di XClarity Administrator).
- Se si utilizza DHCP per assegnare dinamicamente gli indirizzi IP, è necessario configurare l'indirizzo MAC.
- Se si utilizzano indirizzi IP statici, è necessario configurare le seguenti impostazioni di rete per un server specifico prima di poter distribuire un sistema operativo a tale server. Dopo aver configurato tali impostazioni, lo stato di distribuzione delle modifiche del server viene modificato in "Pronto". Alcuni campi non sono disponibili per gli indirizzi IPv6 statici.
  - Nome host

    Il nome host deve essere conforme alle seguenti regole:
    - Il nome host di ciascun server gestito deve essere univoco.
    - Il nome host può contenere stringhe (etichette) separate da un punto (.).
    - Ogni etichetta può contenere lettere, numeri e trattini (-) ASCII; tuttavia, la stringa non può iniziare o terminare con un trattino e non può contenere solo numeri.
    - La prima etichetta può avere una lunghezza compresa tra 2 e 15 caratteri. Le etichette successive possono avere una lunghezza compresa tra 2 e 63 caratteri.
    - La lunghezza totale del nome host non deve superare i 255 caratteri.
  - L'indirizzo MAC della porta sull'host in cui deve essere installato il sistema operativo.

    L'indirizzo MAC è impostato su AUTO per impostazione predefinita. Questa impostazione rileva automaticamente le porte Ethernet che possono essere configurate e utilizzate per la distribuzione. Il primo indirizzo MAC (porta) rilevato viene utilizzato per impostazione predefinita. Se viene rilevata la connettività su un indirizzo MAC differente, l'host XClarity Administrator viene riavviato automaticamente per utilizzare l'indirizzo MAC appena rilevato per la distribuzione.

    È possibile determinare lo stato della porta dell'indirizzo MAC utilizzata per la distribuzione del sistema operativo dal menu a discesa **Indirizzo MAC** nella finestra di dialogo Impostazioni di rete. Se sono presenti più porte o se tutte le porte sono disattivate, viene utilizzato AUTO per impostazione predefinita.

    Nota:

    - Le porte di rete virtuali non sono supportate. Non utilizzare una porta di rete fisica per simulare più porte di rete virtuali.
    - Quando l'impostazione di rete del server è configurata su AUTO, XClarity Administrator può rilevare automaticamente le porte di rete negli slot 1-16. Almeno una porta negli slot 1-16 deve disporre di una connessione a XClarity Administrator.
    - Se si desidera utilizzare una porta di rete nello slot 17 o superiore per l'indirizzo MAC, non è possibile utilizzare l'opzione AUTO. È necessario invece configurare l'impostazione di rete del server con l'indirizzo MAC della porta specifica che si desidera utilizzare.
    - Per i server ThinkServer, non tutti gli indirizzi MAC host sono visualizzati. In molti casi, gli indirizzi MAC per gli adattatori Ethernet AnyFabric sono elencati nella finestra di dialogo Modifica impostazioni di rete. Gli indirizzi MAC per gli altri adattatori Ethernet (ad es. Lan-On-Motherboard) non sono elencati. Nei casi in cui l'indirizzo MAC per un adattatore non è disponibile, utilizzare il metodo AUTO per le distribuzioni non VLAN.
  - Indirizzo IP e maschera di sottorete
  - Gateway IP
  - Fino a due server DNS (Domain Name System)
  - Velocità MTU (Maximum Transmission Unit)

  - ID VLAN, se la modalità IP VLAN è abilitata
- Se si decide di utilizzare VLAN, è possibile assegnare un ID VLAN alla scheda di rete host configurata.

Per ulteriori informazioni sulla rete di distribuzione del sistema operativo e sulle interfacce, vedere Configurazione delle impostazioni di rete per i server gestiti, Configurazione delle impostazioni di rete per i server gestiti e Considerazioni sulla rete nella documentazione online di XClarity Administrator.

Considerazioni su storage e opzioni di avvio

- Prima di distribuire un sistema operativo, verificare che l'opzione di avvio UEFI sul server di destinazione sia impostata su "Solo avvio UEFI". Le opzioni di avvio "Solo legacy" e "Prima UEFI, poi legacy" non sono supportate per la distribuzione del sistema operativo.
- Ciascun server deve essere dotato di un adattatore RAID hardware installato e configurato.

  Attenzione:

  - È supportato solo lo storage configurato con RAID hardware.
  - Il software RAID generalmente presente sull'adattatore di storage SATA Intel integrato o lo storage configurato come JBOD non è supportato. Tuttavia, se non è presente un adattatore RAID hardware, in alcuni casi potrebbe essere possibile abilitare la modalità **SATA AHCI** dell'adattatore SATA per la distribuzione del sistema operativo oppure impostare i dischi validi non configurati su JBOD. Per ulteriori informazioni, vedere Il programma di installazione del sistema operativo non riesce a trovare il disco su cui si desidera installare XClarity Administrator nella documentazione online di XClarity Administrator.

    Questa eccezione non si applica alle unità M.2.
  - Se un dispositivo gestito dispone di entrambe le unità locali (SATA, SAS o SSD) non configurate per la modalità RAID hardware e per le unità M.2, è necessario disabilitare le unità locali se si desidera utilizzare l'unità M.2 oppure è necessario disabilitare le unità M.2 se si desidera utilizzare le unità locali. È possibile disabilitare i dispositivi del controller di storage integrato e le ROM dell'opzione di storage UEFI e legacy mediante i pattern di configurazione, selezionando "Disabilita disco locale" nella scheda "Storage locale" della procedura guidata o creando un pattern di configurazione da un server esistente e quindi disabilitando i dispositivi M.2 nel pattern UEFI esteso.
  - Se è abilitato un adattatore SATA, la modalità SATA *non deve* essere impostata su "IDE."
- Lo storage NVMe non è connesso a una scheda madre del server o il controller HBA non è supportato e non deve essere installato nel dispositivo. In caso contrario, la distribuzione del sistema operativo sullo storage non NVMe avrà esito negativo.
- Durante la distribuzione di RHEL le porte multiple connesse allo stesso LUN sullo storage di destinazione non sono supportate.
- Verificare che la modalità di avvio sicuro sia disabilitata per il server. Se si sta distribuendo un sistema operativo con la modalità di avvio sicuro abilitata (Windows, ad esempio), disabilitare la modalità di avvio sicuro, distribuire il sistema operativo, quindi riabilitare la modalità di avvio sicuro.
- Quando si distribuisce Microsoft Windows su un server, le unità collegate non devono disporre di partizioni di sistema esistenti (vedere La distribuzione del sistema operativo non riesce a causa di partizioni di sistema esistenti su un'unità disco collegata nella documentazione online di XClarity Administrator).
- Per i server ThinkServer, accertarsi che siano rispettati i seguenti requisiti:
  - Le impostazioni di avvio sul server devono includere criteri OpROM di storage impostati su `UEFI Only`. Per ulteriori informazioni, vedere Impossibile avviare il programma di installazione del sistema operativo su un server ThinkServer - XClarity Administrator nella documentazione online di XClarity Administrator.
  - Se si sta distribuendo ESXi e sono presenti adattatori di rete con avvio PXE, disabilitare il supporto PXE degli adattatori di rete prima di distribuire il sistema operativo. La distribuzione è stata completata: è possibile riabilitare il supporto PXE, se desiderato.

– Se si distribuendo ESXi e sono presenti periferiche avviabili nell'elenco dell'ordine di avvio diverse dall'unità su cui deve essere installato il sistema operativo, rimuovere le periferiche avviabili dall'elenco dell'ordine di avvio prima di distribuire il sistema operativo. Una volta completata la distribuzione, è possibile aggiungere nuovamente la periferica avviabile all'elenco. Verificare che l'unità installata sia la prima dell'elenco.

Per ulteriori informazioni sulle impostazioni delle posizioni dello storage, vedere Scelta della posizione di storage per i server gestiti.

Considerazioni sui dispositivi gestiti

- Per informazioni sulle limitazioni della distribuzione del sistema operativo per dispositivi, vedere Supporto XClarity Administrator - Pagina Web sulla compatibilità, fare clic sulla scheda **Compatibilità** e selezionare il collegamento per i tipi di dispositivo appropriati.
- Verificare che non sia montato alcun supporto (ad esempio, ISO) sul server di destinazione. Assicurarsi inoltre che non siano attive sessioni di supporti remoti sul controller di gestione.
- Assicurarsi che il timestamp del BIOS sia impostato su data e ora correnti.
- Per i server con XCC2 con Protezione del sistema abilitato e l'azione impostata su **Impedisci avvio del sistema operativo**, verificare che Protezione del sistema sia conforme sul dispositivo. Se Protezione del sistema non è conforme, ai dispositivi viene impedito il completamento del processo di avvio, determinando un errore della distribuzione del sistema operativo. Per eseguire il provisioning di questi dispositivi, rispondere manualmente al prompt di avvio di Protezione del sistema per consentire l'avvio normale dei dispositivi.
- Per i server ThinkSystem e System x, verificare che l'opzione BIOS legacy sia disabilitata. Da Setup Utility del BIOS/UEFI (F1), fare clic su **Configurazione UEFI → Impostazioni di sistema** e verificare che l'opzione BIOS legacy sia impostata su Disabilitato.
- Per i server Flex System, verificare che lo chassis sia acceso.
- Verificare che una chiave FoD (Feature on Demand) per la presenza remota sia installata sui server Converged, NeXtScale e System x. È possibile determinare se la presenza remota è abilitata, disabilitata o non installata su un server dalla pagina Server (vedere Visualizzazione dello stato di un server gestito). Per ulteriori informazioni sulle chiavi FoD installate nei server, vedere Visualizzazione delle chiavi Features on Demand.
- Per i server ThinkSystem e le appliance ThinkAgile, è richiesta la funzione XClarity Controller Enterprise per la distribuzione del sistema operativo. Per ulteriori informazioni, vedere Visualizzazione delle chiavi Features on Demand.
- Per le appliance Converged e ThinkAgile si consiglia di *non* utilizzare XClarity Administrator per eseguire una distribuzione del sistema operativo bare metal.

Sistemi operativi supportati

Lenovo XClarity Administrator supporta la distribuzione di diversi sistemi operativi. Solo le versioni supportate dei sistemi operativi possono essere caricate nel XClarity Administrator repository di immagini del sistema operativo.

Importante:

- Per informazioni sulle limitazioni della distribuzione del sistema operativo per dispositivi, vedere Supporto XClarity Administrator - Pagina Web sulla compatibilità, fare clic sulla scheda **Compatibilità** e selezionare il collegamento per i tipi di dispositivo appropriati.
- La funzione di gestione della crittografia di XClarity Administrator consente la comunicazione delle limitazioni di determinate modalità SSL/TLS minime. Ad esempio, se si seleziona TLS 1.2, solo i sistemi operativi con un processo di installazione che supporta TLS 1.2 e algoritmi di crittografia avanzati possono essere distribuiti tramite XClarity Administrator.

- Le immagini del sistema operativo nel repository di XClarity Administrator potrebbero non essere supportate solo su determinate piattaforme hardware. Solo i profili immagine del sistema operativo supportati dal server selezionato sono elencati nella pagina "Distribuisci immagini sistema operativo". È possibile determinare se un sistema operativo è compatibile con un server specifico da Sito Web della guida all'interoperabilità del sistema operativo Lenovo.
- Per informazioni sul supporto e la relativa compatibilità di Hypervisor e sistema operativo e sulle risorse per le soluzioni e i server Lenovo, vedere Pagina Web del centro di supporto del sistema operativo del server.

La seguente tabella riporta i sistemi operativi a 64 bit che possono essere distribuiti da XClarity Administrator.

Sistema operativo	Versioni	Note
CentOS Linux	7.2 and later 8.0 8.1 8.2	**Nota:** • Tutte le versioni minori esistenti e future sono supportate se non diversamente indicato. • Sono supportati gli indirizzi DHCP, IPv4 statici e IPv6 statici. • Etichettatura VLAN non supportata. • I driver esterni non sono supportati. • La personalizzazione del profilo del sistema operativo non è supportata. • CentOS 8.3 non è supportato.
Azure Stack HCI di Microsoft® Windows®	20H2 21H2	La personalizzazione del profilo del sistema operativo non è supportata.
Client Microsoft Windows	10 21H2 10 22H2 11 22H2	
Microsoft Windows Server	2012 R2 2012 R2U1 2016 2019 2022	Sono supportate le copie per attivazione singola e multilicenza. **Nota:** XClarity Administrator è stato testato solo con le versioni di Windows supportate da Microsoft al momento del rilascio della versione di XClarity Administrator. I seguenti sistemi *non sono supportati*: • Windows Reseller Option Kit (ROK) • Windows Server Semi-Annual Channel (SAC) v1709, v1803 e v1809 • Windows Server 2019 Essentials • Windows Server 2016 Nanoserver • Copia di valutazione di Windows Server 2012 • Immagini di Windows Server su server gestiti con chiavi di hypervisor incorporato Windows Server 2012 R2 sui server con processori Intel CLX È necessario rimuovere fisicamente la chiave dai server di destinazione prima di distribuire un'immagine Windows. Ciò include Hyper-V tramite uno dei profili di virtualizzazione. – Datacenter – Core del data center – Virtualizzazione del data center (Hyper-V) – Core di virtualizzazione del data center (Hyper-V con core) – Standard – Core standard – Virtualizzazione standard (Hyper-V) – Core di virtualizzazione standard (Hyper-V con core)

Sistema operativo	Versioni	Note
Red Hat® Enterprise Linux (RHEL) Server	6.8 and later 7.2 and later 8.x 9.x	Include KVM **Nota:** • Tutte le versioni minori esistenti e future sono supportate se non diversamente indicato. • Quando si importa la versione DVD dell'immagine del sistema operativo, è supportato solo DVD1. • Quando si installa RHEL sui server ThinkSystem, è consigliato RHEL v7.4 o versioni successive. • Per distribuire RHEL 7.2, l'assegnazione globale degli IP deve essere configurata per utilizzare gli indirizzi IPv4. Per informazioni sulle impostazioni globali, vedere Configurazione delle impostazioni globali di distribuzione del sistema operativo. • Gli errori di distribuzione del sistema operativo sono stati analizzati sulle reti IPv6 con larghezza di banda ridotta a causa dei timeout del programma di installazione del sistema operativo. • Etichettatura VLAN non supportata.
Rocky Linux	8.x 9.x	**Nota:** • Tutte le versioni minori esistenti e future sono supportate se non diversamente indicato. • Sono supportati gli indirizzi DHCP, IPv4 statici e IPv6 statici. • Etichettatura VLAN non supportata. • I driver esterni non sono supportati.
SUSE® Linux Enterprise Server (SLES)	12.x 15.x	Include gli hypervisor Xen e KVM **Nota:** • Tutti i service pack esistenti e futuri sono supportati se non diversamente indicato. • Quando si importa la versione DVD dell'immagine del sistema operativo, è supportato solo DVD1. • Gli errori di distribuzione del sistema operativo sono stati analizzati sulle reti IPv6 con larghezza di banda ridotta a causa dei timeout del programma di installazione del sistema operativo. • Su un server ThinkSystem, se si intende distribuire SLES 12 SP2, è necessario utilizzare un profilo kISO. Per ottenere i profili kISO, è necessario importare l'immagine kISO SLES appropriata. Per ulteriori informazioni, vedere Considerazioni sulla distribuzione del sistema operativo. • Per SLES 15 e 15 SP1, è necessario importare sia l'immagine del programma di installazione sia l'immagine del pacchetto associato dal Pagina Web del centro di supporto del sistema operativo del server. Per SLES 15 SP2 o versione successiva, è necessario importare solo l'immagine del supporto di installazione completa, poiché i DVD dei pacchetti e del programma di installazione unificato di SUSE Linux Enterprise Server 15 e 15 SP1 sono deprecati. • Etichettatura VLAN non supportata.

Sistema operativo	Versioni	Note
Server Ubuntu	20.04.x 22.04.x	**Nota:** • L'immagine può essere installata nell'opzione di storage selezionata (unità disco locale, unità M.2 o volume SAN FC). • Tutte le versioni minori esistenti e future sono supportate se non diversamente indicato. • Solo il DHCP è supportato. Gli indirizzi IPv4 e IPv6 statici *non sono* supportati. • L'etichettatura VLAN *non è* supportata. • I driver esterni *non sono* supportati. • La personalizzazione del profilo del sistema operativo *non è* supportata.
VMware vSphere® Hypervisor (ESXi)	5.5 5.5u1 5.5u2 5.5u3 6.0.x 6.5.x 6.7.x 7.0.x 8.0.x	Le immagini base di VMware vSphere Hypervisor (ESXi) e le immagini di Lenovo VMware ESXi Custom sono supportate. Le immagini Lenovo VMware ESXi Custom sono personalizzate per determinati hardware, in modo da fornire la gestione online della piattaforma, con aggiornamenti e configurazione del firmware, diagnostica della piattaforma e avvisi hardware avanzati. Gli strumenti di gestione Lenovo supportano inoltre la gestione semplificata di ESXi con alcuni server System x. Questa immagine è disponibile per il download da Supporto VMware - Pagina Web dei download. La licenza fornita con l'immagine è una versione di prova gratuita di 60 giorni. L'utente sarà responsabile della soddisfazione di tutti i requisiti di licenza VMware. **Importante:** • Tutti i pacchetti di aggiornamento esistenti e futuri per le versioni 6.0, 6.5, 6.7, 7.0 e 8.0 sono supportati se non diversamente indicato. • Le immagini ESXi base (senza personalizzazione Lenovo) includono solo i driver di dispositivo integrati per rete e storage. L'immagine base non include i driver di dispositivo più recenti (inclusi nelle immagini Lenovo VMware ESXi personalizzate). È possibile aggiungere i driver di dispositivo più recenti creando profili OS0image personalizzati (vedere Personalizzazione dei profili delle immagini del sistema operativo). • Per alcune versioni delle immagini Lenovo VMware ESXi Custom potrebbero essere disponibili immagini separate per System x, ThinkSystem e ThinkServer. Nel repository delle immagini del sistema operativo, può essere presente solo un'immagine per ogni specifica versione. • La distribuzione di ESXi non è supportata per alcuni server più vecchi. Per ulteriori informazioni sui server supportati, vedere Sito Web della guida all'interoperabilità del sistema operativo Lenovo. • Per i dispositivi ThinkServer sono supportate le seguenti versioni: ESXi 6.0u3, 6.5 e versioni successive. • Durante l'installazione di ESXi 5.5 (qualsiasi aggiornamento) o 6.0 su un server in uno chassis di Flex System, il server potrebbe non rispondere o riavviarsi subito dopo il seguente messaggio: `Caricamento image.pld` • VMware ESXi 5.5 richiede la configurazione dello spazio MMIO (Memory Mapped I/O) nei 4 GB iniziali del sistema. A seconda della configurazione, alcuni sistemi tentano di utilizzare più di 4 GB di memoria. Ciò potrebbe causare un errore. Per risolvere il problema, vedere Blocco o riavvio del sistema causato dalla distribuzione VMware nella documentazione online di XClarity Administrator. • Quando si distribuisce ESXi mediante la modalità IPv6 statico, il nome host definito nella pagina "Impostazioni di rete" in XClarity Administrator non è configurato nell'istanza ESXi distribuita. Di contro, viene utilizzato il nome

Sistema operativo	Versioni	Note
		host predefinito `localhost`. È necessario impostare manualmente il nome host nell'istanza ESXi distribuita in modo che corrisponda al nome host definito in XClarity Administrator. • Quando si distribuisce ESXi su un server gestito, il sistema operativo non sposta in modo esplicito l'unità su cui è installato il sistema operativo alla prima voce dell'elenco dell'ordine di avvio. Se un dispositivo di avvio che contiene un server PXE o un sistema operativo avviabile viene specificato prima del dispositivo di avvio che contiene ESXi, ESXi non si avvia. Per la distribuzione di ESXi, XClarity Administrator aggiorna l'elenco dell'ordine di avvio per la maggior parte dei server, al fine di verificare che il dispositivo di avvio ESXi sia il primo nell'elenco dell'ordine di avvio; tuttavia, i server ThinkServer non dispongono di una funzionalità che consenta a XClarity Administrator di aggiornare l'elenco dell'ordine di avvio. Prima di distribuire il sistema operativo è necessario disabilitare il supporto di avvio PXE oppure rimuovere le periferiche avviabili diverse dall'unità di installazione. Per ulteriori informazioni, vedere Il sistema operativo non si avvia dopo avere distribuito ESXi su un server ThinkServer nella documentazione online di XClarity Administrator. **Suggerimento:** anziché impostare **MM Config** tramite Setup Utility per ciascun server, valutare la possibilità di utilizzare uno dei pattern UEFI estesa predefiniti relativi alla virtualizzazione, che imposta l'opzione MM Config su 3 GB e disabilita l'assegnazione di risorse PCI a 64 bit. Per ulteriori informazioni su questi pattern, vedere Definizione delle impostazioni UEFI estese.

Profili immagine del sistema operativo

Quando si importa un'immagine del sistema operativo in repository di immagini del sistema operativo, Lenovo XClarity Administrator crea una o più profili per l'immagine e memorizza i profili in repository di immagini del sistema operativo. Ogni *profilo* predefinito include l'immagine del sistema operativo e le opzioni di installazione dell'immagine.

Attributi del profilo immagine sistema operativo

Gli attributi del profilo immagine sistema operativo forniscono informazioni aggiuntive su un profilo immagine del sistema operativo. Possono essere visualizzati i seguenti attributi.

- **kISO**. È necessario utilizzare un profilo kISO per distribuire SLES 12 SP2 su un server ThinkSystem. È possibile scaricare l'immagine kISO SLES da Supporto Linux - Pagina Web dei download.

Profili predefiniti immagine del sistema operativo

La seguente tabella elenca i profili predefiniti da XClarity Administrator quando si importa un'immagine del sistema operativo. Questa tabella elenca inoltre i pacchetti inclusi in ogni profilo.

È possibile creare un profilo immagine del sistema operativo personalizzato per un sistema operativo di base. Per ulteriori informazioni, vedere Personalizzazione dei profili delle immagini del sistema operativo.

Sistema operativo	profilo	Pacchetti inclusi nel profilo	
CentOS Linux	Base	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Minimo	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Virtualizzazione	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Azure Stack HCI di Microsoft® Windows®	Azure	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="Containers" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />	
Client Microsoft Windows	Enterprise		
	Enterprise N		
	Workstations Pro		
	Workstations_Pro N		

Sistema operativo	profilo	Pacchetti inclusi nel profilo
Microsoft Windows Hyper-V Server 2016	Hyper_V	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />
Microsoft Windows Server **Nota:** Include Hyper-V tramite il *profilo di virtualizzazione*.	Datacenter	GUI
	Virtualizzazione del datacenter	GUI Hyper-V role
	Core di virtualizzazione del datacenter	Hyper-V role
	Core del data center	
	Standard	GUI
	Virtualizzazione standard	GUI Hyper-V role
	Core di virtualizzazione standard	Hyper-V role
	Core standard	
Microsoft Windows Server personalizzato	Datacenter_ customized	
	Standard_ customized	
Red Hat Enterprise Linux (RHEL) **Nota:** Include KVM	Base	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686
	Minimo	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686

Sistema operativo	profilo	Pacchetti inclusi nel profilo	
	Virtualizzazione	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Rocky Linux	Base	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Minimo	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Virtualizzazione	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms

Sistema operativo	profilo	Pacchetti inclusi nel profilo
SUSE Linux Enterprise Server (SLES) 15	Base e base	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Minimo e minimo	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Virtualizzazione - KVM e virtualizzazione - KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
	Virtualizzazione - Xen e virtualizzazione - Xen	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
Ubuntu	Minimo	Openssh-server

Sistema operativo	profilo	Pacchetti inclusi nel profilo
	Virtualizzazione	qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager
VMware vSphere® Hypervisor (ESXi)	Virtualizzazione	Le immagini base di VMware vSphere Hypervisor (ESXi) e le immagini di Lenovo VMware ESXi Custom sono supportate.

Disponibilità della porta per i sistemi operativi distribuiti

Alcune porte sono bloccate da determinati profili di sistema operativo. Nelle seguenti tabelle sono riportate le porte che devono essere aperte (non bloccate).

Comunicazioni	Profilo di virtualizzazione RHEL, Centos e Rocky[1]	Profili RHEL, Centos, Rocky Basic e minimi[1]	Virtualizzazione SLES, profili minimi e di base[2]	Virtualizzazione Ubuntu e profili minimi[3]	Profilo di virtualizzazione VMware ESXi[4]	Profili Windows
In uscita (porte aperte sui sistemi esterni)	• Comunicazione con i dispositivi di rete KVM RHEL: TCP e UDP sulle porte **53** e **67** • Comunicazione con gli agenti SNMP: UDP sulla porta **161** • Comunicazione con l'agente di servizio SLP, l'agente di directory SLP: TCP e UDP sulla porta **427** • Comunicazione CIM-XML su HTTP: TCP sulle porte **15988** e **15989** • Comunicazione del server virtuale KVM: TCP sulle porte **49152 - 49215**					• Comunicazione SMB: TCP sulla porta **445**
In ingresso (porte aperte sull'appliance XClarity	• SSH: TCP sulla porta **22** • Dispositivi di rete KVM RHEL: TCP e UDP sulle porte **53** e **67** • Agenti SNMP: UDP	• SSH: TCP sulla porta **22** • Distribuzione del sistema operativo: TCP e UDP sulle porte **445, 3900** e **8443**	• Distribuzione del sistema operativo: TCP e UDP sulle porte **445, 3900** e **8443**	• Distribuzione del sistema operativo: TCP e UDP sulle porte **445, 3900** e **8443**	• Distribuzione del sistema operativo: TCP e UDP sulle porte **445, 3900** e **8443**	• Distribuzione del sistema operativo: TCP e UDP sulle porte **445, 3900** e **8443**

Co-muni-cazio-ni	Profilo di virtualizzazio-ne RHEL, Centos e Rocky[1]	Profili RHEL, Centos, Rocky Basic e minimi[1]	Virtualizzazio-ne SLES, profili minimi e di base[2]	Virtualizzazio-ne Ubuntu e profili minimi[3]	Profilo di virtualizzazio-ne VMware ESXi[4]	Profili Windows
Admi-nistra-tor)	sulla porta **162** • Distribuzione del sistema operativo: TCP e UDP sulle porte **445, 3900** e **8443** • Agente di servizio SLP, l'agente di directory SLP: TCP e UDP sulla porta **427** • Server virtuale KVM: TCP sulle porte **49152 - 49215**					

1. Per impostazione predefinita, i profili RHEL (Red Hat Enterprise Linux) bloccano tutte le porte, tranne quelle riportate nella seguente tabella.
2. Per SLES (SUSE Linux Enterprise Server), alcune porte aperte vengono assegnate dinamicamente in base a versione e profili del sistema operativo. Per un elenco completo delle porte aperte, consultare la documentazione di SUSE Linux Enterprise Server.
3. Per il server Ubuntu Linux, alcune porte aperte vengono assegnate dinamicamente in base a versione e profili del sistema operativo. Per un elenco completo delle porte aperte, consultare la documentazione del server Ubuntu.
4. Per un elenco completo delle porte aperte di VMware vSphere Hypervisor (ESXi) con personalizzazione Lenovo, consultare la documentazione VMware di ESXi su Sito Web della knowledge base di VMware.

Configurazione di un file server remoto

È possibile importare le immagini sistema operativo, i driver di dispositivo e i file di avvio nel repository di immagini sistema operativo dal sistema locale o da un file server remoto. Per importare i file da un file server remoto, è necessario creare innanzitutto un profilo utilizzato per autenticare la connessione al file server remoto.

Informazioni su questa attività

Sono supportati i seguenti algoritmi di crittografia:
- RSA-2048 bit
- RSA-4096 bit
- ECDSA-521 bit (curva secp521r1)

Sono supportati i seguenti protocolli:
- HTTP senza autenticazione.
- HTTP senza autenticazione di base.

- HTTPS (convalida del certificato) con autenticazione di base.
- HTTPS (convalida del certificato) senza autenticazione.
- FTP con autenticazione password.
- SFTP (convalida client) con autenticazione password.
- SFTP (convalida client) con autenticazione chiave pubblica

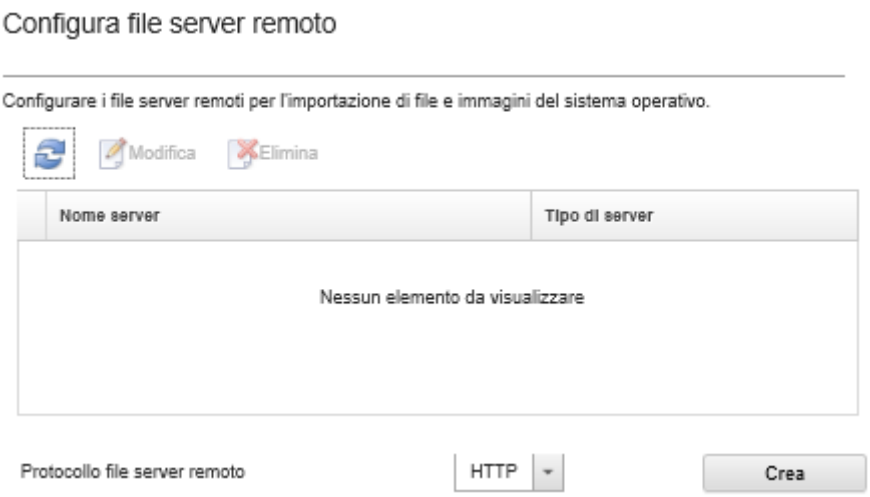
Per l'autenticazione della chiave pubblica SFTP e la convalida del certificato HTTPS, Lenovo XClarity Administrator convalida il certificato del file server remoto. Se il certificato server non è nell'archivio attendibile, verrà richiesto di accettare il certificato server e di aggiungerlo all'archivio attendibile. Per ulteriori informazioni sulla risoluzione dei problemi di convalida, vedere Convalida della certificazione del server non riuscita nella documentazione online di XClarity Administrator.

Procedura

Per configurare un file server remoto, effettuare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.

Passo 2. Fare clic sull'icona **Configura file server** ( ) per visualizzare la finestra di dialogo Configura file server remoto .



Passo 3. Selezionare il protocollo per il file server remoto dall'elenco **Protocollo file server remoto**.

Passo 4. Fare clic su **Crea**. Viene visualizzata la finestra di dialogo "Configura file server remoto".

Nota: Questa finestra di dialogo differisce a seconda del protocollo selezionato.

Passo 5. Immettere il nome del server, l'indirizzo e la porta.

Passo 6. Se per accedere al server è richiesta l'autenticazione, per HTTP, HTTPS, FTP e SFTP con autenticazione di base, immettere un nome utente e una password.

Passo 7. Per SFTP con autenticazione di base, fare clic su **Convalida certificato server** per ottenere la firma della chiave pubblica.

Nota: Potrebbe essere visualizzata una finestra di dialogo in cui si informa che il processo di distribuzione del sistema operativo non considera attendibile la chiave pubblica del file server SFTP. Fare clic su **OK** per memorizzare e considerare attendibile la chiave pubblica SFTP nell'archivio di chiavi attendibili per la distribuzione del sistema operativo. Se l'operazione riesce, la firma della chiave pubblica viene visualizzata nel campo **Firma chiave pubblica server SFTP**.

Passo 8. Per SFTP con autenticazione della chiave pubblica:

a. Se per accedere al server è richiesta l'autenticazione, immettere la passphrase della chiave e la password e selezionare il tipo di chiave.
b. Fare clic su **Genera chiave del server di gestione** per ottenere la firma della chiave pubblica.
c. Copiare la chiave generata nel file delle chiavi autorizzate sul file server SFTP remoto.
d. Selezionare la casella di controllo **La chiave di gestione è stata copiata nel server** in XClarity Administrator.
e. Fare clic su **Convalida certificato server** per convalidare la firma della chiave pubblica.

   Nota: Potrebbe essere visualizzata una finestra di dialogo in cui si informa che il processo di distribuzione del sistema operativo non considera attendibile la chiave pubblica del file server SFTP. Fare clic su **OK** per memorizzare e considerare attendibile la chiave pubblica SFTP nell'archivio di chiavi attendibili per la distribuzione del sistema operativo. Se l'operazione riesce, la firma della chiave pubblica viene visualizzata nel campo **Firma chiave pubblica server SFTP**.
f. Fare clic su **Salva**.

Passo 9. Fare clic su **Salva server**.

Al termine

Dalla finestra di dialogo Configura file server remoto, è possibile eseguire le seguenti operazioni:

- Aggiornare l'elenco del file server remoto facendo clic sull'icona **Aggiorna** ().
- Modificare un file server remoto selezionato facendo clic sull'icona **Modifica** ().
- Rimuovere un file server remoto selezionato facendo clic sull'icona **Elimina** ().

Importazione delle immagini del sistema operativo

Prima di poter distribuire un sistema operativo con licenza sui server gestiti, è necessario importare l'immagine in XClarity Administrator repository di immagini del sistema operativo.

Informazioni su questa attività

Per informazioni sulle immagini del sistema operativo che è possibile importare e distribuire, vedere Sistemi operativi supportati.

Per un elenco dei sistemi operativi di base e personalizzati supportati, vedere Sistemi operativi supportatiSistemi operativi supportati nella documentazione online di Lenovo XClarity Administrator.

È possibile importare solo un'immagine alla volta. Attendere che l'immagine sia visualizzata nel repository di immagini del sistema operativo prima di tentare l'importazione di un'altra immagine. L'importazione del sistema operativo potrebbe richiedere del tempo.

Solo per ESXi, è possibile importare più immagini ESXi con la stessa versione principale/minore nel repository delle immagini del sistema operativo.

Solo per ESXi, è possibile importare più immagini ESXi personalizzate con la stessa versione principale/minore e lo stesso numero di build nel repository delle immagini del sistema operativo.

Durante l'importazione di un'immagine del sistema operativo, XClarity Administrator:

- Verifica che ci sia spazio sufficiente nel repository di immagini del sistema operativo prima di importare il sistema operativo. Se non si dispone di spazio sufficiente per l'importazione di un'immagine, eliminare un'immagine esistente dal repository e tentare di importare nuovamente la nuova immagine.
- Crea uno o più profili dell'immagine e memorizza il profilo nel repository di immagini del sistema operativo. Ciascun *profilo* include l'immagine del sistema operativo e le opzioni di installazione. Per ulteriori informazioni sui profili predefiniti dell'immagine del sistema operativo, vedere Profili immagine del sistema operativo.

Nota: I browser Internet Explorer e Microsoft Edge hanno un limite di caricamento di 4 GB. Se il file da importare è maggiore di 4 GB, considerare la possibilità di utilizzare un altro browser Web (come Chrome o Firefox) oppure copiare il file in un file server remoto e importarlo utilizzando l'opzione **Importazione remota**.

Procedura

Per importare un'immagine del sistema operativo nel repository di immagini del sistema operativo, completare le seguenti operazioni.

Passo 1. Procurarsi un'immagine ISO del sistema operativo con licenza.

Nota: l'utente sarà responsabile dell'acquisizione delle licenze applicabili per il sistema operativo.

Passo 2. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistemi operativi: gestisci immagini sistema operativo.

Passo 3. Fare clic sull'icona **Importa file** () per visualizzare la finestra di dialogo Importa file e immagini del sistema operativo.

Passo 4. Fare clic sulla scheda **Locale** per caricare i file dal sistema locale oppure fare clic sulla scheda **Remoto** per caricare i file da un file server remoto.

Nota: per caricare un file da un file server remoto, è necessario prima creare un profilo del file server remoto, facendo clic sull'icona **Configura file server** (). Per ulteriori informazioni, vedere Configurazione di un file server remoto .

Passo 5. Se si sceglie di utilizzare un file server remoto, selezionare il server che si desidera utilizzare dall'elenco **File server remoto**.

Passo 6. Immettere il percorso e il nome del file dell'immagine ISO oppure fare clic su **Sfoglia** per individuare l'immagine ISO che si desidera importare.

Se si sceglie di utilizzare il *file server locale*, è necessario immettere il percorso assoluto al file di immagine ISO. Se si sceglie di utilizzare un *file server remoto*, è necessario immettere il percorso assoluto (ad esempio, `/home/user/isos.osimage.iso`) o il percorso relativo (ad esempio, `/isos.osimage.iso`) al file di immagine ISO (a seconda della configurazione del file server remoto). Se non è possibile trovare il file, verificare che il percorso del file sia corretto e riprovare.

Passo 7. **Facoltativo:** immettere una descrizione per l'immagine del sistema operativo.

Passo 8. **Facoltativo:** selezionare un tipo di checksum per verificare che l'immagine ISO importata in XClarity Administrator non sia danneggiata, quindi copiare e incollare il valore di checksum nel campo di testo fornito.

Se si seleziona un tipo di checksum, è necessario specificare un valore di checksum per verificare l'integrità e la sicurezza dell'immagine del sistema operativo caricata. Il valore deve provenire da una un'origine sicura, da un'organizzazione attendibile. Se l'immagine caricata corrisponde al valore di checksum, è possibile continuare la distribuzione in tutta sicurezza. Altrimenti, è necessario caricare nuovamente l'immagine oppure controllare il valore di checksum.

Sono supportati tre tipi di checksum:

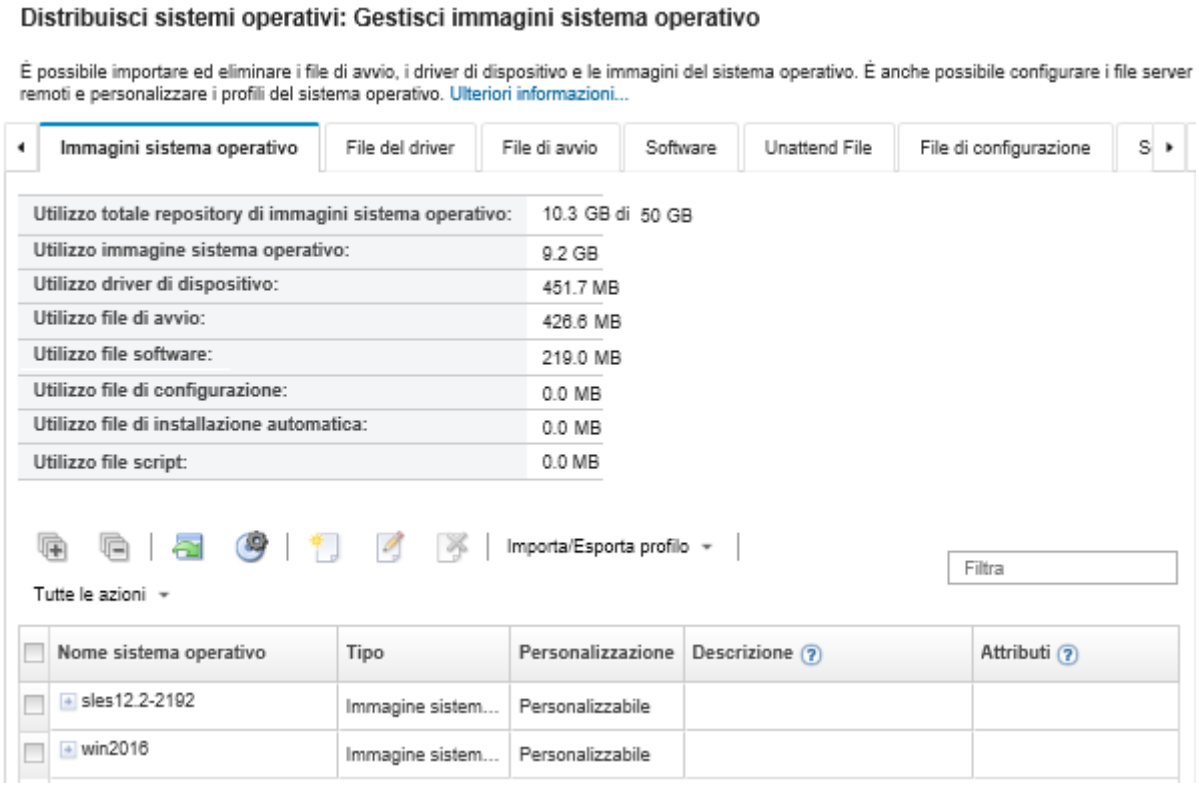
- **MD5**
- **SHA1**
- **SHA256**

Passo 9. Fare clic su **Importa**.

Suggerimento: l'immagine ISO viene caricata su una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione dell'immagine. Se si chiude la scheda o la finestra del browser Web in cui si sta caricando l'immagine del sistema operativo prima del completamento del caricamento, l'importazione non riesce.

Risultati

XClarity Administrator carica l'immagine del sistema operativo e crea un profilo dell'immagine nel repository di immagini del sistema operativo.



Da questa pagina, è possibile completare le seguenti azioni.

- Creare un profilo file server remoto, facendo clic sull'icona **Configura file server** ( ).
- Personalizzare un'immagine del sistema operativo, facendo clic sull'icona **Crea profilo personalizzato** ( ).
- Modificare un'immagine del sistema operativo, facendo clic sull'icona **Modifica** ( ).
- Importare un profilo immagine del sistema operativo personalizzato e applicarlo a un'immagine del sistema operativo di base facendo clic su **Importa/esporta profilo → Importa immagine del profilo personalizzato** (vedere Importazione di un profilo immagine del sistema operativo personalizzato).
- Eliminare un'immagine del sistema operativo selezionata o un profilo immagine del sistema operativo personalizzato facendo clic sull'icona **Elimina** ( ).

- Esportare un profilo immagine del sistema operativo personalizzato selezionato facendo clic su **Importa/esporta profilo → Esporta immagine del profilo personalizzato**.

Nota: Quando si importano le immagini di Windows Server, è necessario importare anche il file del bundle associato. Lenovo fornisce un bundle che include il file di avvio WinPE_64.wim predefinito e un set di driver di dispositivo in un unico pacchetto che può essere scaricato da Pagina Web dei driver di Windows Lenovo e del repository delle immagini WinPE e quindi importato nel repository delle immagini del sistema operativo. Poiché il file del bundle contiene sia i driver di dispositivo sia i file di avvio, è possibile importare il file del bundle dalla scheda **Driver di dispositivo** o **File di avvio**.. Per ulteriori informazioni, vedere Importazione dei file di avvio e Importazione dei driver di dispositivo.

Personalizzazione dei profili delle immagini del sistema operativo

Un *sistema operativo di base* è l'immagine completa del sistema operativo importata nel repository di immagini del sistema operativo. L'immagine di base importata contiene i profili predefiniti che descrivono le configurazioni di installazione per l'immagine. Inoltre, è possibile creare profili personalizzati nell'immagine del sistema operativo di base, che possono essere distribuiti per configurazioni specifiche. Il profilo personalizzato contiene i file personalizzati e le opzioni di installazione.

Nota: Non è possibile creare un profilo dell'immagine del sistema operativo personalizzato per un'immagine di Microsoft Windows Server personalizzata.

Diversi scenari di esempio per la personalizzazione e la distribuzione delle immagini del sistema operativo, come Windows e SLES, sono disponibili solo in inglese. Per ulteriori informazioni, vedere Scenari end-to-end per configurare nuovi dispositivi.

È possibile aggiungere i seguenti tipi di file a un profilo dell'immagine del sistema operativo.

- **File di avvio**

  Un file di avvio viene utilizzato come ambiente di installazione bootstrap. Per Windows, questo è un file di preinstallazione di Windows (WinPE). Per distribuire Windows è richiesto un file di avvio WinPE.

  Lenovo XClarity Administrator supporta file di avvio predefiniti e personalizzati.

  – **File di avvio predefiniti**. Lenovo fornisce un file di avvio WinPE_64.wim che può essere utilizzato per distribuire i profili immagine del sistema operativo predefiniti.

    Lenovo fornisce un bundle che include il file di avvio WinPE_64.wim predefinito e un set di driver di dispositivo in un unico pacchetto che può essere scaricato da Pagina Web dei driver di Windows Lenovo e del repository delle immagini WinPE e quindi importato nel repository delle immagini del sistema operativo. Poiché il file del bundle contiene sia i driver di dispositivo sia i file di avvio, è possibile importare il file del bundle dalla scheda **Driver di dispositivo** o **File di avvio**.

    Nota:

    – Un file di avvio predefinito non è precaricato con XClarity Administrator. Prima di poter distribuire un profilo Windows, è necessario importare un file di avvio nel repository di immagini del sistema operativo.

    – Non è possibile eliminare i file di avvio predefiniti, caricati quando è installato XClarity Administrator. Tuttavia, è possibile eliminare i file di avvio predefiniti importati da un bundle Lenovo.

    – XClarity Administrator richiede che i file importati del bundle siano firmati da Lenovo. Durante l'importazione di un file del bundle, è necessario importare anche un file delle firme .asc.

  – **File di avvio personalizzati**. È possibile creare un file di avvio di WinPE per personalizzare le opzioni di avvio per una distribuzione di Windows. È quindi possibile aggiungere il file di avvio ai profili Windows personalizzati.

XClarity Administrator fornisce script per la creazione dei file di avvio nel formato corretto. Per ulteriori informazioni sulla creazione dei file di avvio personalizzati, vedere Creazione di un file di avvio (WinPE) e Sito Web sull'introduzione a Windows PE (WinPE).

Per l'importazione dei file di avvio personalizzati sono supportati i seguenti tipi di file.

Sistema operativo	Tipi di file di avvio supportati	Tipi di file del bundle supportati
CentOS Linux	Non supportato	Non supportato
Azure Stack HCI di Microsoft® Windows®	Non supportato	Non supportato
Microsoft Windows Hyper-V Server	Un file .zip che contiene un file WinPE creato utilizzando lo script **genimage.cmd**	Un file .zip che contiene i driver di dispositivo e i file di avvio
Microsoft Windows Server	Un file .zip che contiene un file WinPE creato utilizzando lo script **genimage.cmd**	Un file .zip che contiene i driver di dispositivo e i file di avvio
Red Hat® Enterprise Linux (RHEL) Server	Non supportato	Non supportato
Rocky Linux	Non supportato	Non supportato
SUSE® Linux Enterprise Server (SLES)	Non supportato	Non supportato
Ubuntu	Non supportato	Non supportato
VMware vSphere® Hypervisor (ESXi) con Lenovo Customization	Non supportato	Non supportato

- **Driver di dispositivo**

  Verificare che l'immagine del sistema operativo che si intende distribuire includa i driver di dispositivo dell'adattatore di storage, Fibre Channel ed Ethernet corretti per l'hardware. Se il driver di dispositivo dell'adattatore I/O non è incluso nel profilo o nell'immagine del sistema operativo, l'adattatore non è supportato per la distribuzione del sistema operativo. È possibile creare profili di immagine del sistema operativo personalizzati che comprendono i driver di dispositivo necessari non inclusi.

  Lenovo XClarity Administrator supporta i driver di dispositivo inclusi nonché i driver di dispositivo non inclusi personalizzati e predefiniti.

  – **Driver di dispositivo inclusi**. XClarity Administrator non gestisce driver di dispositivo inclusi. Installare sempre il sistema operativo più recente per accertarsi di possedere gli ultimi driver di dispositivo inclusi necessari.

    Nota: È possibile aggiungere i driver di dispositivo inclusi a un profilo Windows personalizzato creando un file di avvio WinPE personalizzato e copiando i file dei driver di dispositivo nella directory `C:\drivers` del sistema host. Quando si crea un profilo immagine del sistema operativo personalizzato che utilizza il file di avvio personalizzato, i driver di dispositivo presenti nella directory C:\drivers vengono inclusi sia in WinPE sia nel sistema operativo finale. I driver vengono considerati come integrati. Pertanto, non è necessario importare questi driver di dispositivo inclusi in XClarity Administrator, quando si specificano i driver di dispositivo da utilizzare per la creazione del profilo dell'immagine del sistema operativo personalizzato.

  – **Driver di dispositivo predefiniti**. Per i server ThinkSystem, XClarity Administrator è precaricato con un set di driver di dispositivo non inclusi per Linux, in modo da abilitare l'installazione del sistema operativo e la configurazione base di rete e di storage per il sistema operativo finale. È possibile aggiungere questi driver di dispositivo predefiniti ai profili di immagine del sistema operativo personalizzati e distribuire i profili ai server gestiti.

Lenovo fornisce anche bundle dei driver di dispositivo predefiniti in un unico pacchetto che può essere scaricato da Pagina Web dei driver di Windows Lenovo e del repository delle immagini WinPE e quindi importato nel repository delle immagini del sistema operativo. Attualmente, i file del bundle sono disponibili solo per Windows. Se il file del bundle contiene sia i driver di dispositivo sia i file di avvio, è possibile importare il file del bundle dalla scheda **Driver di dispositivo** o **Immagine di avvio**.

Nota:

- Per impostazione predefinita, i profili immagine del sistema operativo predefiniti includono i driver di dispositivo predefiniti.
- Non è possibile eliminare i driver di dispositivo predefiniti, caricati quando è installato XClarity Administrator. Tuttavia, è possibile eliminare i driver di dispositivo predefiniti importati da un bundle Lenovo.
- XClarity Administrator richiede che i file importati del bundle siano firmati da Lenovo. Durante l'importazione di un file del bundle, è necessario importare anche un file delle firme .asc.

- **Driver di dispositivo personalizzati**. È possibile importare i driver di dispositivo non inclusi nel repository di immagini del sistema operativo e quindi aggiungerli a un profilo personalizzato di immagine del sistema operativo.

  È possibile ottenere i driver di dispositivo da Pagina Web di Lenovo YUM Repository, dal fornitore (come Red Hat) oppure tramite un driver di dispositivo personalizzato, creato autonomamente. Per alcuni driver di dispositivo Windows, è possibile generare un driver di dispositivo personalizzato estraendo il driver di dispositivo dal file .exe di installazione nel sistema locale e creando un file di archivio .zip.

  Per l'importazione dei driver di dispositivo personalizzati sono supportati i seguenti tipi di file.

Sistema operativo	Tipi di file di driver di dispositivo supportati
CentOS Linux	Non supportato
Azure Stack HCI di Microsoft® Windows®	Non supportato
Microsoft Windows Hyper-V Server	Un file .zip contenente i file di driver di dispositivo non elaborati, che generalmente sono raggruppati in file .inf, .cat e .dll.
Microsoft Windows Server	Un file .zip contenente i file di driver di dispositivo non elaborati, che generalmente sono raggruppati in file .inf, .cat e .dll.
Red Hat® Enterprise Linux (RHEL) Server	Disco DUD (Driver Update Disk) in formato immagine .rpm o .iso **Nota:** Se si applica un file DUD.rpm al profilo personalizzato, il file .rpm viene installato solo sul sistema operativo finale. Non viene installato nell'ambiente di installazione (initrd). Per installare un driver di dispositivo personalizzato nell'ambiente initrd, importare un file DUD.iso e applicarlo al profilo personalizzato.
Rocky Linux	Non supportato
SUSE® Linux Enterprise Server (SLES)	File DUD (Driver Update Disk) in formato immagine .iso o .rpm **Nota:** Se si applica un file DUD.rpm al profilo personalizzato, il file .rpm viene installato solo sul sistema operativo finale. Non viene installato nell'ambiente di installazione (initrd). Per installare un driver di dispositivo personalizzato nell'ambiente initrd, importare un file DUD.iso e applicarlo al profilo personalizzato.
Ubuntu	Non supportato
VMware vSphere® Hypervisor (ESXi) con Lenovo Customization	Driver di dispositivo in formato immagine .vib

Nota: Il repository di immagini del sistema operativo consente di memorizzare un numero illimitato di file predefiniti e personalizzati, se è disponibile lo spazio per l'archiviazione dei file.

- **Impostazioni di configurazione personalizzate**

  Le impostazioni di configurazione descrivono i dati che devono essere raccolti dinamicamente durante la distribuzione del sistema operativo. Lenovo XClarity Administrator utilizza una serie di impostazioni di configurazione predefinite, come: globale, rete e impostazioni della posizione di storage. È possibile utilizzare queste impostazioni di configurazione predefinite e aggiungere impostazioni di configurazione personalizzate, non disponibili tramite XClarity Administrator.

  Le impostazioni di configurazione personalizzate vengono definite con uno schema JSON. Lo schema deve essere conforme alle specifiche JSON.

  Quando si importano le impostazioni di configurazione personalizzate in XClarity Administrator, XClarity Administrator convalida lo schema JSON. Se la convalida riesce, XClarity Administrator genera macro personalizzate per ogni impostazione.

  È possibile utilizzare le macro personalizzate con il file di installazione automatica e lo script post-installazione.

  Nei file di installazione automatica

  È possibile associare il file di configurazione personalizzato con un file di installazione automatica e includere le macro personalizzate (e predefinite) nel file di installazione automatica.

  È possibile aggiungere uno o più file delle impostazioni di configurazione personalizzate in un profilo personalizzato. Quando si distribuisce il profilo del sistema operativo su una serie di server di destinazione, è possibile scegliere il file delle impostazioni di configurazione da utilizzare. XClarity Administrator visualizza la scheda **Impostazioni personalizzate** nella finestra di dialogo "Distribuisci immagini sistema operativo" in base allo schema JSON nel file delle impostazioni di configurazione e consente di specificare i valori per ogni impostazione (oggetto JSON) definita nel file.

  Nota: La distribuzione del sistema operativo non proseguirà se non viene specificato l'input per le impostazioni di configurazione personalizzate richieste.

  Negli script post-installazione

  Una volta raccolti i dati durante la distribuzione del sistema operativo, XClarity Administrator crea un'istanza del file delle impostazioni di configurazione (che include le impostazioni personalizzate nel file selezionato e un sottoinsieme di impostazioni predefinite) sul sistema host, che può essere utilizzato dallo script post-installazione.

  Nota:

  - Il file delle impostazioni di configurazione è unico per ogni profilo immagine del sistema operativo personalizzato.
  - È possibile modificare le impostazioni di configurazione per i profili immagine del sistema operativo predefinito.
  - Le impostazioni di configurazione sono supportate solo per i sistemi operativi seguenti:
    - Microsoft® Windows® Server
    - Red Hat® Enterprise Linux (RHEL) Server
    - Rocky Linux
    - SUSE® Linux Enterprise Server (SLES)
    - VMware vSphere® Hypervisor (ESXi) con Lenovo Customization 6.0u3 e aggiornamenti successivi e 6.5 e versioni successive.

Il repository di immagini del sistema operativo consente di memorizzare un numero illimitato di file predefiniti e personalizzati, se è disponibile lo spazio per l'archiviazione dei file.

- **File di installazione automatica personalizzati**

  È possibile personalizzare i profili immagine del sistema operativo per utilizzare i file di installazione automatica per automatizzare la distribuzione del sistema operativo.

  Sono supportati i seguenti tipi di file di installazione automatica personalizzati.

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
CentOS Linux	Non supportato	
Azure Stack HCI di Microsoft® Windows®	Non supportato	
Microsoft Windows Hyper-V Server	Non supportato	
Microsoft Windows Server	Installazione automatica (.xml)	Per ulteriori informazioni sui file di installazione automatica, vedere Pagina Web di riferimento per l'installazione automatica di Windows.
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	Per ulteriori informazioni sui file di installazione automatica, vedere Red Hat: pagina Web sull'automazione dell'installazione con Kickstart. Tenere presente quando segue quando si aggiungono le sezioni %pre, %post, %firstboot al file. – È possibile includere più sezioni %pre, %post, %firstboot al file di installazione automatica. In tal caso, prestare attenzione all'ordinamento delle sezioni. – Quando la macro consigliata **#predefined. unattendSettings.preinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge una sezione %pre prima di tutte le altre sezioni %pre nel file. – Quando la macro consigliata **#predefined. unattendSettings.postinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge le sezioni %post e %firstboot prima di tutte le altre sezioni %post e %firstboot nel file.
Rocky Linux	Kickstart (.cfg)	Per ulteriori informazioni sui file di installazione automatica, vedere Red Hat: pagina Web sull'automazione dell'installazione con Kickstart. Tenere presente quando segue quando si aggiungono le sezioni %pre, %post, %firstboot al file. – È possibile includere più sezioni %pre, %post, %firstboot al file di installazione automatica. In tal caso, prestare attenzione all'ordinamento delle sezioni. – Quando la macro consigliata **#predefined. unattendSettings.preinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge una sezione %pre prima di tutte le altre sezioni %pre nel file. – Quando la macro consigliata **#predefined. unattendSettings.postinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge le sezioni %post e %firstboot prima di tutte le altre sezioni %post e %firstboot nel file.

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	Per ulteriori informazioni sui file di installazione automatica, vedere SUSE: pagina Web di AutoYaST.
Ubuntu	Non supportato	
VMware vSphere® Hypervisor (ESXi) con Lenovo Customization	Kickstart (.cfg)	Supportato solo per ESXi 6.0u3 e gli aggiornamenti più recenti, nonché per la versione 6.5 e successive. Per ulteriori informazioni sui file di installazione automatica, vedere VMware: installazione o aggiornamento degli host mediante una pagina Web degli script. Tenere presente quando segue quando si aggiungono le sezioni %pre, %post, %firstboot al file. – È possibile includere più sezioni %pre, %post, %firstboot al file di installazione automatica. In tal caso, prestare attenzione all'ordinamento delle sezioni. – Quando la macro consigliata **#predefined.unattendSettings.preinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge una sezione %pre prima di tutte le altre sezioni %pre nel file. – Quando la macro consigliata **#predefined.unattendSettings.postinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge le sezioni %post e %firstboot prima di tutte le altre sezioni %post e %firstboot nel file.

Attenzione:

– È possibile inserire macro predefinite e personalizzate (impostazioni di configurazione) nel file di installazione automatica utilizzando il nome univoco dell'oggetto. I valori predefiniti sono dinamici in base alle istanze XClarity Administrator. Le macro personalizzate sono dinamiche in base all'input dell'utente, specificato durante la distribuzione del sistema operativo.

  Nota:

  – Racchiudere il nome della macro con il simbolo hash (#).
  – Per gli oggetti nidificati, separare ogni nome dell'oggetto con un punto (ad esempio, **#server_settings.server0.locale#**).
  – Per le macro personalizzate, non includere il nome dell'oggetto principale. Per le macro predefinite, utilizzare un prefisso "predefinito" per il nome della macro.
  – Quando viene creato un oggetto da un modello, il nome viene aggiunto con un numero univoco, a partire da 0 (ad esempio, **server0** e **server1**).
  – È possibile visualizzare il nome per ogni macro dalla finestra di dialogo Distribuisci immagini sistema operativo sulle schede Impostazioni personalizzate, passando il mouse sull'icona Guida () accanto a ciascuna impostazione personalizzata.
  – Per un elenco di macro predefinite, vedere Macro predefinite. Per informazioni sulle impostazioni di configurazione personalizzate e le macro, vedere Macro personalizzate.

– XClarity Administrator fornisce le seguenti macro predefinite utilizzate per comunicare lo stato dal programma di installazione del sistema operativo, nonché altre diverse fasi di installazione critiche. Si consiglia di includere queste macro nel file di installazione automatica (vedere Inserimento di macro predefinite e personalizzate in un file di installazione automatica).
  – #predefined.unattendSettings.preinstallConfig#

  - #predefined.unattendSettings postinstallConfig#

- **Script di installazione personalizzati**

  È possibile personalizzare i profili immagine del sistema operativo per eseguire uno script di installazione, una volta completata la distribuzione del sistema operativo.

  Attualmente, sono supportati solo gli script post-installazione.

  La seguente tabella elenca i tipi di file per gli script di installazione che Lenovo XClarity Administrator supporta per ciascun sistema operativo. Tenere presente che alcune versioni di sistema operativo non supportano tutti i tipi di file che XClarity Administrator supporta (ad esempio, alcune versioni di RHEL potrebbero non includere Perl nel profilo minimi e pertanto gli script Perl non verranno eseguiti). Accertarsi di utilizzare il tipo di file corretto per le versioni del sistema operativo che si desidera distribuire.

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
CentOS Linux	Non supportato	
Azure Stack HCI di Microsoft® Windows®	Non supportato	
Microsoft Windows Hyper-V Server	Non supportato	
Microsoft® Windows® Server	File di comando (.cmd), PowerShell (.ps1)	Il percorso predefinito di file e dati personalizzati è `C:\lxca`. Per ulteriori informazioni sugli script di installazione, vedere Pagina Web sull'aggiunta di uno script personalizzato all'installazione di Windows
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm o .pl), Python (.py)	Il percorso predefinito di file e dati personalizzati è `/home/lxca`. Per ulteriori informazioni sugli script di installazione, vedere RHEL: pagina Web degli script post-installazione.
Rocky Linux	Bash (.sh), Perl (.pm o .pl), Python (.py)	Il percorso predefinito di file e dati personalizzati è `/home/lxca`. Per ulteriori informazioni sugli script di installazione, vedere RHEL: pagina Web degli script post-installazione
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm o .pl), Python (.py)	Il percorso predefinito di file e dati personalizzati è `/home/lxca`. Per ulteriori informazioni sugli script di installazione, vedere SUSE: pagina Web degli script utente personalizzati
Ubuntu	Non supportato	
VMware vSphere® Hypervisor (ESXi) con Lenovo Customization	Bash (.sh), Python (.py)	Il percorso predefinito di file e dati personalizzati è `/home/lxca`. Per ulteriori informazioni sugli script di installazione, vedere VMware: pagina Web degli script di aggiornamento e installazione

- **Software personalizzato**

  È possibile personalizzare i profili immagine del sistema operativo per installare payload del software personalizzati, una volta completati gli script di post-installazione e distribuzione del sistema operativo.

  Sono supportati i seguenti tipi di file per il software personalizzato.

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
CentOS Linux	Non supportato	
Azure Stack HCI di Microsoft® Windows®	Non supportato	
Microsoft Windows Hyper-V Server	Non supportato	
Microsoft Windows® Server	Un file .zip contenente il payload del software.	Il percorso predefinito di file e dati personalizzati è `C:\lxca`.
Red Hat® Enterprise Linux (RHEL) Server	Un file .tar.gz contenente il payload del software	Il percorso predefinito di file e dati personalizzati è `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	Un file .tar.gz contenente il payload del software	Il percorso predefinito di file e dati personalizzati è `/home/lxca`.
Rocky Linux	Un file .tar.gz contenente il payload del software	Il percorso predefinito di file e dati personalizzati è `/home/lxca`.
Ubuntu	Non supportato	
VMware vSphere® Hypervisor (ESXi) con Lenovo Customization	Un file .tar.gz contenente il payload del software	Il percorso predefinito di file e dati personalizzati è `/home/lxca`.

Importazione di un profilo immagine del sistema operativo personalizzato

È possibile importare un profilo immagine del sistema operativo personalizzato e aggiungerlo a un'immagine del sistema operativo di base compatibile esistente.

Informazioni su questa attività

È necessario importare l'immagine del sistema operativo di base, prima di importare un profilo personalizzato.

Un profilo immagine del sistema operativo personalizzato può essere aggiunto solo a un'immagine del sistema operativo di base dello stesso tipo. Ad esempio, se il profilo esportato è per un'immagine Windows 2016, il profilo può essere importato e aggiunto solo a un'immagine di Windows 2016 esistente nel repository di immagini del sistema operativo.

Il repository di immagini del sistema operativo consente di memorizzare un numero illimitato di profili personalizzati, se è disponibile lo spazio per l'archiviazione dei file.

Procedura

Per importare un profilo immagine del sistema operativo personalizzato, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.

Passo 2. Dalla scheda **immagini del sistema operativo**, selezionare l'immagine del sistema operativo di base a cui si desidera aggiungere il profilo immagine del sistema operativo personalizzato.

Passo 3. Fare clic su **Importa/Esporta profilo → Importa immagine del profilo personalizzata**. Viene visualizzata la finestra di dialogo Importa profilo immagine del sistema operativo personalizzata.

Passo 4. Fare clic sulla scheda **Importazione locale** per caricare i file dal sistema locale oppure fare clic sulla scheda **Importazione remota** per scaricare i file da un file server remoto.

Nota: Per caricare un file da un file server remoto, è necessario prima creare un profilo del file server remoto, facendo clic sull'icona **Configura file server** (). Per ulteriori informazioni, vedere Configurazione di un file server remoto .

Passo 5. Se si sceglie di utilizzare un file server remoto, selezionare il server che si desidera utilizzare dall'elenco **File server remoto**.

Passo 6. Immettere il nome del profilo oppure fare clic su **Sfoglia** per individuare il profilo che si desidera importare.

Passo 7. **Facoltativo:** per le importazioni locali, selezionare un tipo di checksum per verificare che il file caricato non sia corrotto e copiare e incollare il valore di checksum nel campo di testo fornito.

Se si seleziona un tipo di checksum, è necessario specificare un valore di checksum per controllare l'integrità e la sicurezza del file caricato. Il valore deve provenire da una un'origine sicura, da un'organizzazione attendibile. Se il file caricato corrisponde al valore di checksum, la distribuzione può essere eseguita in modo sicuro. In caso contrario, è necessario caricare nuovamente il file oppure controllare il valore di checksum.

Sono supportati tre tipi di checksum:
- **MD5**
- **SHA1**
- **SHA256**

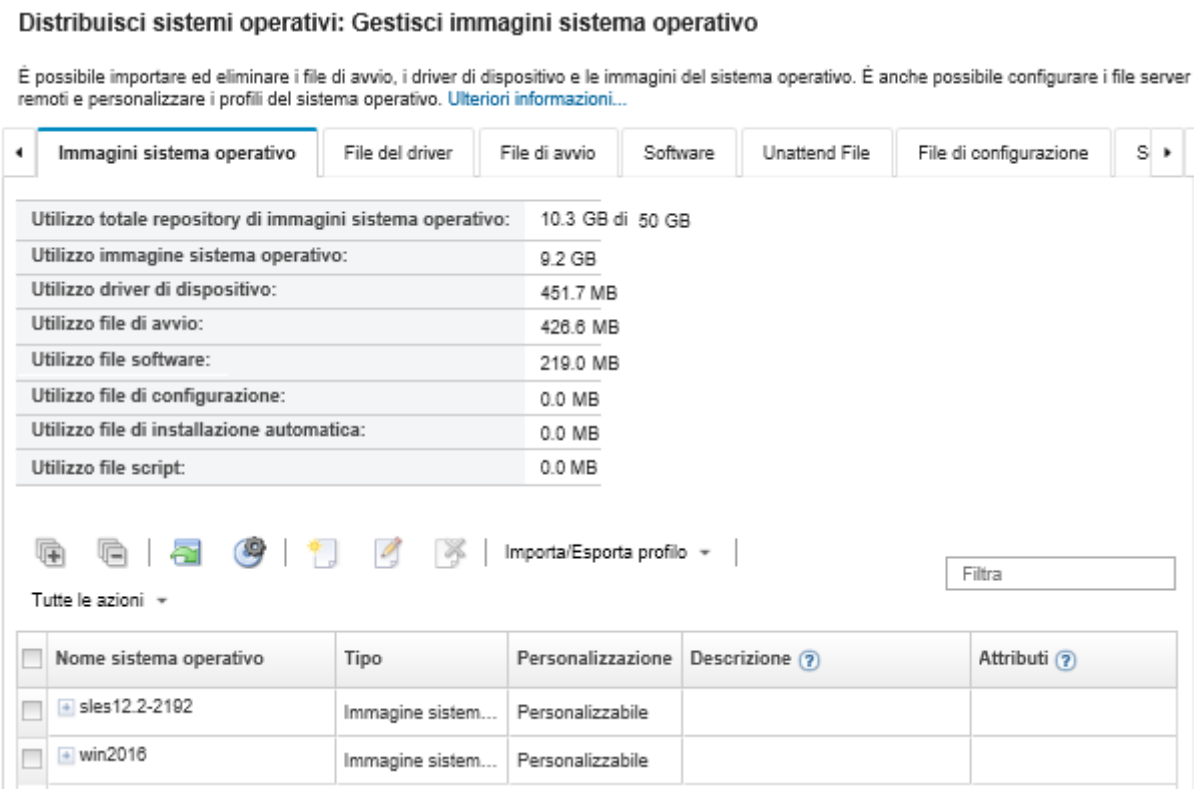
Passo 8. Fare clic su **Importa**.

Suggerimento: il file viene caricato tramite una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione del file.

Se si chiude la scheda o la finestra del browser Web in cui il file viene caricato localmente prima del completamento dell'operazione, l'importazione non riesce.

Al termine

Il profilo immagine del sistema operativo personalizzato viene riportato nel sistema operativo di base nella pagina "Gestisci immagini sistema operativo".



Da questa pagina, è possibile eseguire le seguenti azioni:

- Creare un profilo immagine del sistema operativo personalizzato (vedere Creazione di un profilo immagine del sistema operativo personalizzato).
- Esportare un profilo immagine del sistema operativo personalizzato selezionato, facendo clic su **Importa/esporta profilo → Esporta immagine del profilo personalizzato**.

  Importante: È possibile esportare i profili immagine del sistema operativo personalizzati in un file server remoto configurato per l'utilizzo di protocolli FTP o SFTP. Non è possibile eseguire l'esportazione in un file server remoto configurato per l'utilizzo di HTTP o HTTPS.
- Modificare un profilo personalizzato di immagine del sistema operativo selezionato, facendo clic sull'icona **Modifica** ( ).
- Rimuovere un profilo personalizzato di immagine del sistema operativo selezionato, facendo clic sull'icona **Elimina** ( ).

Importazione dei file di avvio

È possibile importare i file di avvio nel repository di immagini del sistema operativo. Questi file possono quindi essere utilizzati per personalizzare e distribuire le immagini di Windows.

Informazioni su questa attività

Un file di avvio viene utilizzato come ambiente di installazione bootstrap. Per Windows, questo è un file di preinstallazione di Windows (WinPE). Per distribuire Windows è richiesto un file di avvio WinPE.

Lenovo XClarity Administrator supporta file di avvio predefiniti e personalizzati.

- **File di avvio predefiniti**. Lenovo fornisce un file di avvio WinPE_64.wim che può essere utilizzato per distribuire i profili immagine del sistema operativo predefiniti.

Lenovo fornisce un bundle che include il file di avvio WinPE_64.wim predefinito e un set di driver di dispositivo in un unico pacchetto che può essere scaricato da Pagina Web dei driver di Windows Lenovo e del repository delle immagini WinPE e quindi importato nel repository delle immagini del sistema operativo. Poiché il file del bundle contiene sia i driver di dispositivo sia i file di avvio, è possibile importare il file del bundle dalla scheda **Driver di dispositivo** o **File di avvio**.

Nota:

- Un file di avvio predefinito non è precaricato con XClarity Administrator. Prima di poter distribuire un profilo Windows, è necessario importare un file di avvio nel repository di immagini del sistema operativo.
- Non è possibile eliminare i file di avvio predefiniti, caricati quando è installato XClarity Administrator. Tuttavia, è possibile eliminare i file di avvio predefiniti importati da un bundle Lenovo.
- XClarity Administrator richiede che i file importati del bundle siano firmati da Lenovo. Durante l'importazione di un file del bundle, è necessario importare anche un file delle firme .asc.

- **File di avvio personalizzati**. È possibile creare un file di avvio di WinPE per personalizzare le opzioni di avvio per una distribuzione di Windows. È quindi possibile aggiungere il file di avvio ai profili Windows personalizzati.

  XClarity Administrator fornisce script per la creazione dei file di avvio nel formato corretto. Per ulteriori informazioni sulla creazione dei file di avvio personalizzati, vedere Creazione di un file di avvio (WinPE) e Sito Web sull'introduzione a Windows PE (WinPE).

  Per l'importazione dei file di avvio personalizzati sono supportati i seguenti tipi di file.

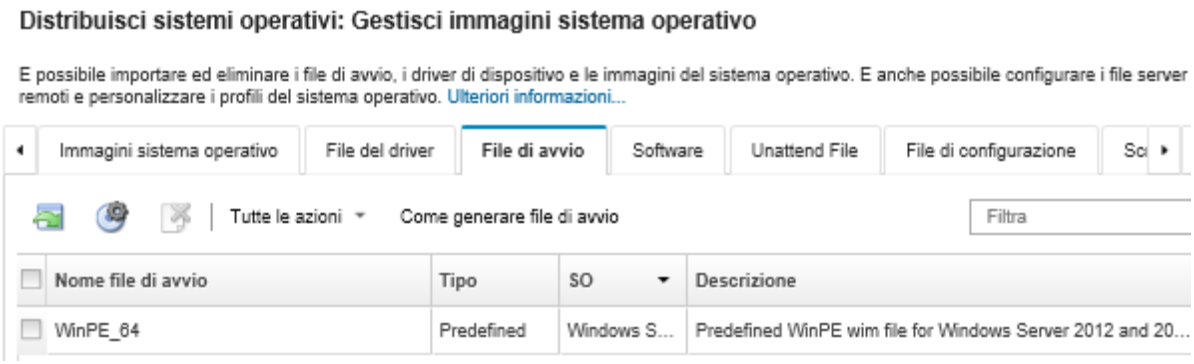
Sistema operativo	Tipi di file di avvio supportati	Tipi di file del bundle supportati
CentOS Linux	Non supportato	Non supportato
Azure Stack HCI di Microsoft® Windows®	Non supportato	Non supportato
Microsoft Windows Hyper-V Server	Un file .zip che contiene un file WinPE creato utilizzando lo script **genimage.cmd**	Un file .zip che contiene i driver di dispositivo e i file di avvio
Microsoft Windows Server	Un file .zip che contiene un file WinPE creato utilizzando lo script **genimage.cmd**	Un file .zip che contiene i driver di dispositivo e i file di avvio
Red Hat® Enterprise Linux (RHEL) Server	Non supportato	Non supportato
Rocky Linux	Non supportato	Non supportato
SUSE® Linux Enterprise Server (SLES)	Non supportato	Non supportato
Ubuntu	Non supportato	Non supportato
VMware vSphere® Hypervisor (ESXi) con Lenovo Customization	Non supportato	Non supportato

Nota: Il repository di immagini del sistema operativo consente di memorizzare un numero illimitato di file predefiniti e personalizzati, se è disponibile lo spazio per l'archiviazione dei file.

Procedura

- Per importare un file del bundle di Windows che contiene i file di avvio nel repository di immagini del sistema operativo, completare le seguenti operazioni.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **File di avvio**.



3. Fare clic su **Scarica → File del bundle di Windows** per accedere alla pagina Web del supporto Lenovo e scaricare nel sistema locale il file del bundle appropriato e il file delle firme associato per l'immagine del sistema operativo.
4. Fare clic sull'icona **Importa file del bundle** ( ). Viene visualizzata la finestra di dialogo Importa file del bundle.
5. Fare clic sulla scheda **Importazione locale** per caricare i file dal sistema locale oppure fare clic sulla scheda **Importazione remota** per scaricare i file da un file server remoto.

   Nota: Per caricare un file da un file server remoto, è necessario prima creare un profilo del file server remoto, facendo clic sull'icona **Configura file server** ( ). Per ulteriori informazioni, vedere Configurazione di un file server remoto .
6. Se si sceglie di utilizzare un file server remoto, selezionare il server che si desidera utilizzare dall'elenco **File server remoto**.
7. Selezionare il tipo e la versione del sistema operativo.
8. Immettere il nome del file del bundle e il file delle firme associato oppure fare clic su **Sfoglia** per individuare i file che si desidera importare.
9. **Facoltativo:** immettere una descrizione per il file del bundle.
10. Fare clic su **Importa**.

    Suggerimento: il file viene caricato tramite una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione del file.

    Se si chiude la scheda o la finestra del browser Web in cui il file viene caricato localmente prima del completamento dell'operazione, l'importazione non riesce.

- Per importare un singolo file di avvio nel repository di immagini del sistema operativo, completare le seguenti operazioni.
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
  2. Fare clic sulla scheda **File di avvio**.
  3. Fare clic sull'icona **Importa file** ( ). Viene visualizzata la finestra di dialogo Importa file.
  4. Fare clic sulla scheda **Importazione locale** per caricare i file dal sistema locale oppure fare clic sulla scheda **Importazione remota** per scaricare i file da un file server remoto.

Nota: Per caricare un file da un file server remoto, è necessario prima creare un profilo del file server remoto, facendo clic sull'icona **Configura file server** (). Per ulteriori informazioni, vedere Configurazione di un file server remoto .

5. Se si sceglie di utilizzare un file server remoto, selezionare il server che si desidera utilizzare dall'elenco **File server remoto**.
6. Selezionare il tipo e la versione del sistema operativo.
7. Immettere il nome del file oppure fare clic su **Sfoglia** per individuare il file di avvio che si desidera importare.
8. **Facoltativo:** immettere una descrizione per il file di avvio.
9. **Facoltativo:** selezionare un tipo di checksum per verificare che il file caricato non sia danneggiato e copiare e incollare il valore di checksum nel campo di testo fornito.

   Se si seleziona un tipo di checksum, è necessario specificare un valore di checksum per controllare l'integrità e la sicurezza del file caricato. Il valore deve provenire da una un'origine sicura, da un'organizzazione attendibile. Se il file caricato corrisponde al valore di checksum, la distribuzione può essere eseguita in modo sicuro. In caso contrario, è necessario caricare nuovamente il file oppure controllare il valore di checksum.

   Sono supportati tre tipi di checksum:
   - **MD5**
   - **SHA1**
   - **SHA256**
10. Fare clic su **Importa**.

    Suggerimento: il file viene caricato tramite una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione del file.

    Se si chiude la scheda o la finestra del browser Web in cui il file viene caricato localmente prima del completamento dell'operazione, l'importazione non riesce.

Al termine

Il file di avvio viene riportato nella scheda **File di avvio** nella pagina Gestisci immagini sistema operativo.

Da questa pagina, è possibile completare le seguenti azioni.

- Creare un profilo file server remoto, facendo clic sull'icona **Configura file server** ().
- Rimuovere un file di avvio selezionato facendo clic sull'icona **Elimina** ().
- Aggiungere un file di avvio a un profilo immagine del sistema operativo personalizzato (vedere Creazione di un profilo immagine del sistema operativo personalizzato).

Creazione di un file di avvio (WinPE)

È possibile creare file di avvio da utilizzare per personalizzare le immagini di Windows.

Prima di iniziare

- Verificare che il sistema operativo di cui si intende effettuare il provisioning sia installato sull'host. Ad esempio, se si prevede di effettuare il provisioning di Windows 2016 utilizzando i file di WinPE, installare Windows 2016 sull'host.
- Verificare che Microsoft ADK compatibile con il sistema operativo installato sia anche installato sull'host. Ad esempio, Windows 2012R2 richiede l'aggiornamento ADK versione 8.1.
- Ottenere i driver di dispositivo, in formato .inf, da aggiungere al file di avvio.

È possibile ottenere i driver di dispositivo da Pagina Web di Lenovo YUM Repository, dal fornitore (come Red Hat) oppure tramite un driver di dispositivo personalizzato, creato autonomamente. Per alcuni driver di dispositivo Windows, è possibile generare un driver di dispositivo personalizzato estraendo il driver di dispositivo dal file .exe di installazione nel sistema locale e creando un file di archivio .zip.

Lenovo fornisce anche bundle dei driver di dispositivo predefiniti in un unico pacchetto che può essere scaricato da Pagina Web dei driver di Windows Lenovo e del repository delle immagini WinPE e quindi importato nel repository delle immagini del sistema operativo. Attualmente, i file del bundle sono disponibili solo per Windows. Se il file del bundle contiene sia i driver di dispositivo sia i file di avvio, è possibile importare il file del bundle dalla scheda **Driver di dispositivo** o **Immagine di avvio**.

- Scaricare i file `genimage.cmd` e `startnet.cmd` nell'host all'interno di una directory temporanea come `C:\customwim`.

  Il comando `genimage.cmd` viene utilizzato per generare i file di avvio di WinPE, come il file .wim. Il comando `startnet.cmd` viene utilizzato da XClarity Administrator per il bootstrap di Windows Installer.
- Decidere come si desidera inserire i driver di dispositivo nel file di avvio. È possibile eseguire questa operazione utilizzando uno dei seguenti metodi:
  - Aggiungere i driver di dispositivo inclusi a un profilo Windows personalizzato copiando i file dei driver di dispositivo nella directory C:\drivers del sistema host. Questi verranno inclusi nel file di avvio quando il comando "genimage.cmd" viene eseguito in un secondo momento.

    Nota: Quando si crea un profilo immagine del sistema operativo personalizzato che utilizza il file di avvio personalizzato, i driver di dispositivo presenti nella directory C:\drivers vengono inclusi sia in WinPE sia nel sistema operativo finale. I driver vengono considerati come integrati. Pertanto, non è necessario importare questi driver di dispositivo inclusi in XClarity Administrator, quando si specificano i driver di dispositivo da utilizzare per la creazione del profilo dell'immagine del sistema operativo personalizzato.
  - Aggiungere i driver di dispositivo esclusi direttamente al file di avvio.

    Nota: Se si utilizza questo metodo, i driver di dispositivo vengono applicati esclusivamente al file di avvio e pertanto all'ambiente di installazione WinPE. I driver di dispositivo non vengono applicati al sistema operativo finale installato. È necessario importare manualmente i driver di dispositivo nel repository dei driver di dispositivo delle immagini del sistema operativo e selezionarli per utilizzarli nell'ambito della personalizzazione del profilo immagine del sistema operativo.
- Per ulteriori informazioni sui file di avvio, vedere Sito Web sull'introduzione a Windows PE (WinPE).

Procedura

Per creare un file di avvio, attenersi alla procedura descritta di seguito.

Passo 1. Utilizzando un ID utente con autorità di amministratore, eseguire il comando di Windows ADK "Deployment and Imaging Tools Environment". Verrà visualizzata una sessione del comando.

Passo 2. Dalla sessione del comando passare alla directory in cui i file `genimage.cmd` e `starnet.cmd` sono stati scaricati (ad esempio, `C:\customwim`).

Passo 3. Verificare che nell'host non siano presenti immagini precedentemente montate eseguendo il comando seguente:

```
dism /get-mountedwiminfo
```

Se sono presenti immagini montate, rimuoverle eseguendo il comando seguente:

```
dism /unmount-wim /MountDir:C:\<mount_path> /Discard
```

Passo 4. Se si aggiungono driver di dispositivo inclusi a un profilo Windows personalizzato, copiare i file dei driver di dispositivo non elaborati, in formato .inf, nella directory `C:\drivers` del sistema host.

Passo 5. Eseguire il comando seguente per generare il file di avvio, in formato .wim, e attendere per alcuni minuti il completamento del comando.
`genimage.cmd amd64 <ADK_Version>`

Dove *<ADK_Version>* è uno dei seguenti valori.

- **8.1**. Per Windows 2012 R2
- **10**. Per Windows 2016

Questo comando crea il file di avvio: `C:\WinPE_64\media\Boot\WinPE_64.wim`.

Passo 6. Montare il file di avvio eseguendo il comando seguente:
`DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount`

Passo 7. Se si aggiungono i driver di dispositivo non inclusi direttamente al file di avvio, attenersi alla procedura descritta di seguito.

1. Creare la seguente struttura di directory, dove *<os_release>* è `2012`, `2012R2` o `2016`
`drivers\<os_release>\`
2. Copiare i driver di dispositivo, in formato .inf, in una directory all'interno di tale percorso, ad esempio:
`drivers\<os_release>\<driver1>\<driver1_files>`
3. Copiare la directory `drivers` nella directory di montaggio, ad esempio:
`C:\WinPE_64\mount\drivers`

Passo 8. Apportare ulteriori personalizzazioni al file di avvio, come l'aggiunta di cartelle, file, script di avvio, language pack e applicazioni. Per ulteriori informazioni sulla personalizzazione dei file di avvio, vedere WinPE: sito Web sul montaggio e la personalizzazione.

Passo 9. Smontare l'immagine eseguendo il comando seguente.
`DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit`

Passo 10. Comprimere il contenuto della directory `C:\WinPE_64\media` in un file zip denominato `WinPE_64.zip`.

Passo 11. Importare il file .zip in XClarity Administrator (vedere Importazione dei file di avvio).

Importazione dei driver di dispositivo

È possibile importare singoli driver di dispositivo e file dei bundle nel repository delle immagini del sistema operativo. Questi file possono quindi essere utilizzati per personalizzare le immagini di Linux e Windows.

Informazioni su questa attività

Verificare che l'immagine del sistema operativo che si intende distribuire includa i driver di dispositivo dell'adattatore di storage, Fibre Channel ed Ethernet corretti per l'hardware. Se il driver di dispositivo dell'adattatore I/O non è incluso nel profilo o nell'immagine del sistema operativo, l'adattatore non è supportato per la distribuzione del sistema operativo. È possibile creare profili di immagine del sistema operativo personalizzati che comprendono i driver di dispositivo necessari non inclusi.

Lenovo XClarity Administrator supporta i driver di dispositivo inclusi nonché i driver di dispositivo non inclusi personalizzati e predefiniti.

- **Driver di dispositivo inclusi**. XClarity Administrator non gestisce driver di dispositivo inclusi. Installare sempre il sistema operativo più recente per accertarsi di possedere gli ultimi driver di dispositivo inclusi necessari.

  Nota: È possibile aggiungere i driver di dispositivo inclusi a un profilo Windows personalizzato creando un file di avvio WinPE personalizzato e copiando i file dei driver di dispositivo nella directory `C:\drivers` del sistema host. Quando si crea un profilo immagine del sistema operativo personalizzato che utilizza il file di avvio personalizzato, i driver di dispositivo presenti nella directory C:\drivers vengono inclusi sia in WinPE

sia nel sistema operativo finale. I driver vengono considerati come integrati. Pertanto, non è necessario importare questi driver di dispositivo inclusi in XClarity Administrator, quando si specificano i driver di dispositivo da utilizzare per la creazione del profilo dell'immagine del sistema operativo personalizzato.

- **Driver di dispositivo predefiniti**. Per i server ThinkSystem, XClarity Administrator è precaricato con un set di driver di dispositivo non inclusi per Linux, in modo da abilitare l'installazione del sistema operativo e la configurazione base di rete e di storage per il sistema operativo finale. È possibile aggiungere questi driver di dispositivo predefiniti ai profili di immagine del sistema operativo personalizzati e distribuire i profili ai server gestiti.

  Lenovo fornisce anche bundle dei driver di dispositivo predefiniti in un unico pacchetto che può essere scaricato da Pagina Web dei driver di Windows Lenovo e del repository delle immagini WinPE e quindi importato nel repository delle immagini del sistema operativo. Attualmente, i file del bundle sono disponibili solo per Windows. Se il file del bundle contiene sia i driver di dispositivo sia i file di avvio, è possibile importare il file del bundle dalla scheda **Driver di dispositivo** o **Immagine di avvio**.

  Nota:

  – Per impostazione predefinita, i profili immagine del sistema operativo predefiniti includono i driver di dispositivo predefiniti.

  – Non è possibile eliminare i driver di dispositivo predefiniti, caricati quando è installato XClarity Administrator. Tuttavia, è possibile eliminare i driver di dispositivo predefiniti importati da un bundle Lenovo.

  – XClarity Administrator richiede che i file importati del bundle siano firmati da Lenovo. Durante l'importazione di un file del bundle, è necessario importare anche un file delle firme .asc.

- **Driver di dispositivo personalizzati**. È possibile importare i driver di dispositivo non inclusi nel repository di immagini del sistema operativo e quindi aggiungerli a un profilo personalizzato di immagine del sistema operativo.

  È possibile ottenere i driver di dispositivo da Pagina Web di Lenovo YUM Repository, dal fornitore (come Red Hat) oppure tramite un driver di dispositivo personalizzato, creato autonomamente. Per alcuni driver di dispositivo Windows, è possibile generare un driver di dispositivo personalizzato estraendo il driver di dispositivo dal file .exe di installazione nel sistema locale e creando un file di archivio .zip.

  Per l'importazione dei driver di dispositivo personalizzati sono supportati i seguenti tipi di file.

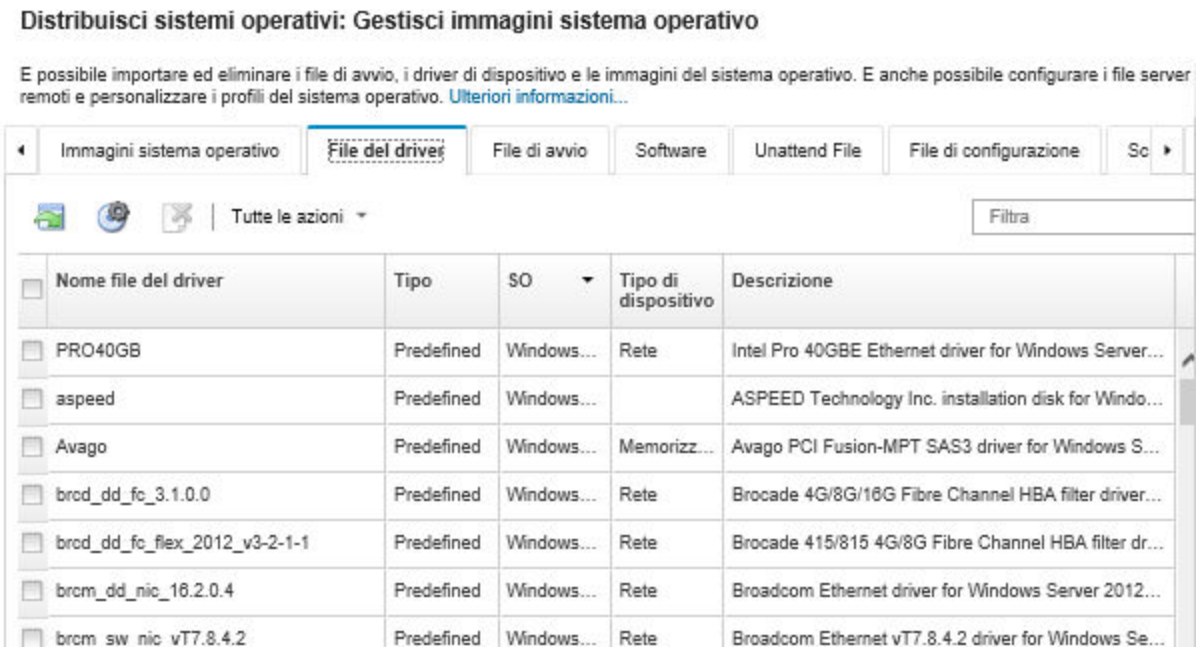
Sistema operativo	Tipi di file di driver di dispositivo supportati
CentOS Linux	Non supportato
Azure Stack HCI di Microsoft® Windows®	Non supportato
Microsoft Windows Hyper-V Server	Un file .zip contenente i file di driver di dispositivo non elaborati, che generalmente sono raggruppati in file .inf, .cat e .dll.
Microsoft Windows Server	Un file .zip contenente i file di driver di dispositivo non elaborati, che generalmente sono raggruppati in file .inf, .cat e .dll.
Red Hat® Enterprise Linux (RHEL) Server	Disco DUD (Driver Update Disk) in formato immagine .rpm o .iso **Nota:** Se si applica un file DUD.rpm al profilo personalizzato, il file .rpm viene installato solo sul sistema operativo finale. Non viene installato nell'ambiente di installazione (initrd). Per installare un driver di dispositivo personalizzato nell'ambiente initrd, importare un file DUD.iso e applicarlo al profilo personalizzato.
Rocky Linux	Non supportato

Sistema operativo	Tipi di file di driver di dispositivo supportati
SUSE® Linux Enterprise Server (SLES)	File DUD (Driver Update Disk) in formato immagine .iso o .rpm **Nota:** Se si applica un file DUD.rpm al profilo personalizzato, il file .rpm viene installato solo sul sistema operativo finale. Non viene installato nell'ambiente di installazione (initrd). Per installare un driver di dispositivo personalizzato nell'ambiente initrd, importare un file DUD.iso e applicarlo al profilo personalizzato.
Ubuntu	Non supportato
VMware vSphere® Hypervisor (ESXi) con Lenovo Customization	Driver di dispositivo in formato immagine .vib

Nota: Il repository di immagini del sistema operativo consente di memorizzare un numero illimitato di file predefiniti e personalizzati, se è disponibile lo spazio per l'archiviazione dei file.

Procedura

- Per importare un file del bundle di Windows che contiene i driver di dispositivo nel repository di immagini del sistema operativo, completare le seguenti operazioni.
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
  2. Fare clic sulla scheda **File del driver**.



  3. Fare clic su **Scarica → File del bundle di Windows** per accedere alla pagina Web del supporto Lenovo e scaricare nel sistema locale il file del bundle appropriato e il file delle firme associato per l'immagine del sistema operativo.
  4. Fare clic sull'icona **Importa file del bundle** ( ). Viene visualizzata la finestra di dialogo Importa file del bundle.
  5. Fare clic sulla scheda **Importazione locale** per caricare i file dal sistema locale oppure fare clic sulla scheda **Importazione remota** per scaricare i file da un file server remoto.

Nota: Per caricare un file da un file server remoto, è necessario prima creare un profilo del file server remoto, facendo clic sull'icona **Configura file server** (). Per ulteriori informazioni, vedere Configurazione di un file server remoto .

6. Se si sceglie di utilizzare un file server remoto, selezionare il server che si desidera utilizzare dall'elenco **File server remoto**.
7. Selezionare il tipo e la versione del sistema operativo.
8. Immettere il nome del file del bundle e il file delle firme associato oppure fare clic su **Sfoglia** per individuare i file che si desidera importare.
9. **Facoltativo:** immettere una descrizione per il file del bundle.
10. Fare clic su **Importa**.

    Suggerimento: il file viene caricato tramite una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione del file.

    Se si chiude la scheda o la finestra del browser Web in cui il file viene caricato localmente prima del completamento dell'operazione, l'importazione non riesce.

- Per importare un singolo driver di dispositivo nel repository di immagini del sistema operativo, completare le seguenti operazioni.
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
  2. Fare clic sulla scheda **File del driver**.
  3. Fare clic sull'icona **Importa file** (). Viene visualizzata la finestra di dialogo Importa file.
  4. Fare clic sulla scheda **Importazione locale** per caricare i file dal sistema locale oppure fare clic sulla scheda **Importazione remota** per scaricare i file da un file server remoto.

     Nota: Per caricare un file da un file server remoto, è necessario prima creare un profilo del file server remoto, facendo clic sull'icona **Configura file server** (). Per ulteriori informazioni, vedere Configurazione di un file server remoto .
  5. Se si sceglie di utilizzare un file server remoto, selezionare il server che si desidera utilizzare dall'elenco **File server remoto**.
  6. Selezionare il tipo e la versione del sistema operativo.
  7. Immettere il nome del file oppure fare clic su **Sfoglia** per individuare il driver di dispositivo che si desidera importare.
  8. **Facoltativo:** immettere una descrizione per il driver di dispositivo.
  9. **Facoltativo:** selezionare un tipo di checksum per verificare che il file caricato non sia danneggiato e copiare e incollare il valore di checksum nel campo di testo fornito.

     Se si seleziona un tipo di checksum, è necessario specificare un valore di checksum per controllare l'integrità e la sicurezza del file caricato. Il valore deve provenire da una un'origine sicura, da un'organizzazione attendibile. Se il file caricato corrisponde al valore di checksum, la distribuzione può essere eseguita in modo sicuro. In caso contrario, è necessario caricare nuovamente il file oppure controllare il valore di checksum.

     Sono supportati tre tipi di checksum:
     - **MD5**
     - **SHA1**
     - **SHA256**
  10. Fare clic su **Importa**.

Suggerimento: il file viene caricato tramite una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione del file.

Se si chiude la scheda o la finestra del browser Web in cui il file viene caricato localmente prima del completamento dell'operazione, l'importazione non riesce.

Al termine

L'immagine del driver del dispositivo viene riportata nella scheda **File del driver** nella pagina Gestisci immagini sistema operativo.

Da questa pagina, è possibile completare le seguenti azioni.

- Creare un profilo file server remoto, facendo clic sull'icona **Configura file server** ( ).
- Rimuovere il driver di dispositivo selezionato facendo clic sull'icona **Elimina** ( ).
- Aggiungere un driver di dispositivo a un profilo immagine del sistema operativo personalizzato (vedere Creazione di un profilo immagine del sistema operativo personalizzato).

Importazione delle impostazioni di configurazione personalizzate

Le impostazioni di configurazione descrivono i dati che devono essere raccolti dinamicamente durante la distribuzione del sistema operativo. Lenovo XClarity Administrator utilizza una serie di impostazioni di configurazione predefinite, come: globale, rete e impostazioni della posizione di storage. È possibile utilizzare queste impostazioni di configurazione predefinite e aggiungere impostazioni di configurazione personalizzate, non disponibili tramite XClarity Administrator.

Informazioni su questa attività

Le impostazioni di configurazione personalizzate vengono definite con uno schema JSON. Lo schema deve essere conforme alle specifiche JSON.

Quando si importano le impostazioni di configurazione personalizzate in XClarity Administrator, XClarity Administrator convalida lo schema JSON. Se la convalida riesce, XClarity Administrator genera macro personalizzate per ogni impostazione.

È possibile utilizzare le macro personalizzate con il file di installazione automatica e lo script post-installazione.

Nei file di installazione automatica

È possibile associare il file di configurazione personalizzato con un file di installazione automatica e includere le macro personalizzate (e predefinite) nel file di installazione automatica.

È possibile aggiungere uno o più file delle impostazioni di configurazione personalizzate in un profilo personalizzato. Quando si distribuisce il profilo del sistema operativo su una serie di server di destinazione, è possibile scegliere il file delle impostazioni di configurazione da utilizzare. XClarity Administrator visualizza la scheda **Impostazioni personalizzate** nella finestra di dialogo "Distribuisci immagini sistema operativo" in base allo schema JSON nel file delle impostazioni di configurazione e consente di specificare i valori per ogni impostazione (oggetto JSON) definita nel file.

Nota: La distribuzione del sistema operativo non proseguirà se non viene specificato l'input per le impostazioni di configurazione personalizzate richieste.

Negli script post-installazione

Una volta raccolti i dati durante la distribuzione del sistema operativo, XClarity Administrator crea un'istanza del file delle impostazioni di configurazione (che include le impostazioni personalizzate nel file selezionato e un sottoinsieme di impostazioni predefinite) sul sistema host, che può essere utilizzato dallo script post-installazione.

Nota:

- Il file delle impostazioni di configurazione è unico per ogni profilo immagine del sistema operativo personalizzato.
- È possibile modificare le impostazioni di configurazione per i profili immagine del sistema operativo predefinito.
- Le impostazioni di configurazione sono supportate solo per i sistemi operativi seguenti:
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - Rocky Linux
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) con Lenovo Customization 6.0u3 e aggiornamenti successivi e 6.5 e versioni successive.

Il repository di immagini del sistema operativo consente di memorizzare un numero illimitato di file predefiniti e personalizzati, se è disponibile lo spazio per l'archiviazione dei file.

Procedura

Per importare i file delle impostazioni di configurazione nel repository di immagini del sistema operativo, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.

Passo 2. Fare clic sulla scheda **Impostazioni di configurazione**.

Passo 3. Fare clic sull'icona **Importa file** ( ). Verrà visualizzata la finestra di dialogo "Importa impostazioni di configurazione".

Passo 4. Fare clic sulla scheda **Importazione locale** per caricare i file dal sistema locale oppure fare clic sulla scheda **Importazione remota** per scaricare i file da un file server remoto.

Nota: Per caricare un file da un file server remoto, è necessario prima creare un profilo del file server remoto, facendo clic sull'icona **Configura file server** ( ). Per ulteriori informazioni, vedere Configurazione di un file server remoto .

Passo 5. Se si sceglie di utilizzare un file server remoto, selezionare il server che si desidera utilizzare dall'elenco **File server remoto**.

Passo 6. Selezionare il tipo di sistema operativo.

Passo 7. Immettere il nome del file delle impostazioni di configurazione oppure fare clic su **Sfoglia** per individuare il file che si desidera importare.

Passo 8. **Facoltativo:** immettere una descrizione delle impostazioni di configurazione.

Suggerimento: utilizzare il campo **Descrizione** per distinguere i file personalizzati con lo stesso nome.

Passo 9. **Facoltativo:** selezionare un tipo di checksum per verificare che il file caricato non sia danneggiato e copiare e incollare il valore di checksum nel campo di testo fornito.

Se si seleziona un tipo di checksum, è necessario specificare un valore di checksum per controllare l'integrità e la sicurezza del file caricato. Il valore deve provenire da una un'origine sicura, da un'organizzazione attendibile. Se il file caricato corrisponde al valore di checksum, la distribuzione può essere eseguita in modo sicuro. In caso contrario, è necessario caricare nuovamente il file oppure controllare il valore di checksum.

Sono supportati tre tipi di checksum:
- **MD5**
- **SHA1**
- **SHA256**

Passo 10. Fare clic su **Importa**. Il formato JSON viene convalidato quando si importa il file. Se vengono rilevati errori, viene visualizzata una finestra di dialogo con il messaggio di errore e la posizione.

Suggerimento: il file viene caricato tramite una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione del file.

Attenzione: Se si chiude la scheda o la finestra del browser Web in cui il file viene caricato localmente prima del completamento dell'operazione, l'importazione non riesce.

Al termine

I file delle impostazioni di configurazione sono elencati nella scheda **Impostazioni di configurazione** nella pagina "Gestisci immagini sistema operativo".

Da questa pagina, è anche possibile completare le seguenti azioni.

- Creare un file delle impostazioni di configurazione facendo clic sull'icona **Crea** ( ) e quindi specificare il nome del file, la descrizione, il tipo del sistema operativo, le impostazioni di configurazione e i valori. Fare clic su **Convalida** per convalidare lo schema prima di salvare il file.

  L'editor identifica la posizione di eventuali errori rilevati nel file. Tenere presente che alcuni messaggi sono solo in inglese.

- Visualizzare e modificare un file delle impostazioni di configurazione facendo clic sull'icona **Modifica** ( ).

  Non è possibile modificare un file delle impostazioni di configurazione associato a un file di installazione automatica.

  L'editor identifica la posizione di eventuali errori rilevati nel file. Tenere presente che alcuni messaggi sono solo in inglese.

- Copiare un file delle impostazioni di configurazione facendo clic sull'icona **Copia** ( ).

  Se si copia un file delle impostazioni di configurazione associato a un file di installazione automatica, viene copiato anche il file di installazione automatica associato e l'associazione tra i due file copiati viene creata automaticamente.

- Rimuovere i file delle impostazioni di configurazione selezionati facendo clic sull'icona **Elimina** ().
- Creare un profilo file server remoto, facendo clic sull'icona **Configura file server** ().

Per informazioni su come aggiungere un file delle impostazioni di configurazione a un profilo immagine del sistema operativo personalizzato, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

Macro personalizzate

Le *macro* forniscono la possibilità di aggiungere dati variabili (impostazioni di configurazione) a un file di installazione automatica o a uno script post-installazione. Lenovo XClarity Administrator consente di definire le impostazioni personalizzate creando un file di impostazioni di configurazione personalizzate, utilizzando il formato JSON.

Il valore per ogni impostazione di configurazione personalizzata varia in base all'input specificato dall'utente durante la distribuzione del sistema operativo.

Quando si importano le impostazioni di configurazione personalizzate in XClarity Administrator, XClarity Administrator convalida lo schema JSON. Se la convalida riesce, XClarity Administrator genera macro personalizzate per ogni impostazione.

Per inserire le macro personalizzate in un file di installazione automatica o in uno script post-installazione, utilizzare il nome univoco dell'oggetto, separare gli oggetti nidificati con un punto e quindi racchiudere il nome della macro con il simbolo hash (#), ad esempio, **#server_settings.server0.locale#**.

Nota:

- Non includere il nome dell'oggetto principale.
- Quando viene creato un oggetto da un modello, il nome viene aggiunto con un numero univoco, a partire da 0 (ad esempio, server0 e server1).
- È possibile visualizzare il nome per ogni macro dalla finestra di dialogo Distribuisci immagini sistema operativo sulle schede Impostazioni personalizzate, passando il mouse sull'icona **Guida** () accanto a ciascuna impostazione personalizzata.

Impostazioni di configurazione

È possibile definire le impostazioni di configurazione personalizzate che:

- Sono comuni a tutti i server di destinazione o univoche per un server di destinazione specifico.
- Dispongono di valori statici (non configurabili) o di valori dinamici (configurabili) immessi quando si distribuisce il profilo immagine del sistema operativo.
- Dispongono di un numero variabile di elementi basato su un modello. Ad esempio, è possibile definire un'impostazione di configurazione che consente di specificare i server NTP 0-3 durante la distribuzione.

Impostazioni comuni

Durante la distribuzione del sistema operativo, gli elementi dell'interfaccia utente delle schede **Impostazioni comuni** della finestra di dialogo "Distribuisci immagine sistema operativo" vengono visualizzati in base agli oggetti rappresentati nell'oggetto **content**. Gli oggetti descrivono le impostazioni e i valori necessari a tutti i server di destinazione per la distribuzione del sistema operativo.

Per rappresentare le impostazioni comuni a tutti i server, il file JSON deve contenere un oggetto principale con un oggetto nidificato che contiene la coppia nome/valore `"common":true`.

Nel seguente esempio vengono utilizzati gli stessi server NTP (dinamici) configurabili per tutti i server.

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": true,
      "description": "NTP Servers",
      "label": "NTP Servers",
      "maxElements": 3,
      "minElements": 0,
      "name": "common-ntpservers",
      "optional": true,
      "template": [{
         "autoCreateInstance": true,
         "category": "dynamic",
         "common": true,
         "description": "A NTP Server",
         "label": "NTP Server",
         "name": "ntpserver",
         "optional": true,
         "regex": "[\\w\\.]{1,64}$",
         "type": "string"
      }],
      "type": "array"
   },
   ...,
}
```

Nel seguente esempio viene utilizzata la stessa directory di log degli script post-installazione (statici) non configurabile.

```
{
   "category": "dynamic",
   "content": [{
      "category": "static",
      "common": true,
      "description": "Directory location for post-installation script logging.",
      "name": "logpath",
      "optional": false,
      "type": "string",
      "value": "/tmp/mylogger.log"
   },
   ...,
}
```

Impostazioni specifiche del server

Durante la distribuzione del sistema operativo, gli elementi dell'interfaccia utente della scheda **Impostazioni specifiche del server** della finestra di dialogo "Distribuisci immagine sistema operativo" vengono visualizzati in base agli oggetti rappresentati nell'oggetto **content** del modello. Gli oggetti descrivono le impostazioni e i valori necessari a un server di destinazione specifico per la distribuzione del sistema operativo.

Una volta raccolti i valori specifici del server nell'interfaccia utente, viene creato un oggetto **content** in formato JSON per ciascun server di destinazione, in base all'oggetto **template**. Ciascun oggetto **content** contiene un campo **name** e **targetServer** univoco e gli eventuali valori specificati per il server.

Per rappresentare le impostazioni specifiche del server, il file JSON deve contenere un oggetto principale con il seguente contenuto:

- La coppia nome/valore `"category":"dynamic"`.

- L'oggetto nidificato che contiene la coppia nome/valore `"common":false`. Solo un oggetto `"common": false` è supportato nel contenuto dell'oggetto principale.
- Un oggetto modello con un oggetto di contenuto integrato. Questo array modello può contenere solo un oggetto.

Ad esempio, se si desidera definire le impostazioni internazionali univoche del sistema operativo per ciascun server di destinazione

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": false,
      "name": "server-settings",
      "optional": false,
      "template": [{
         "category": "dynamic",
         "common": false,
         "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
         }],
         "name": "server",
         "optional": false,
         "type": "assoc_array"
      }],
      "type": "assoc_array"
   },
   ...,
}
```

Specifica JSON

La seguente tabella descrive i campi consentiti dalle specifiche JSON.

Parametro	Obbligatorio/ Facoltativo	Tipo	Descrizione
autoCreateInstance	opzionale	Valore booleano	Indica se un'istanza dell'oggetto modello viene creata automaticamente nel file JSON in fase di distribuzione. É possibile selezionare uno dei seguenti valori. • **true**. Un'istanza dell'oggetto modello viene creata automaticamente nel file JSON in fase di distribuzione. • **false**. (predefinito) Un'istanza dell'oggetto modello *non* viene creata automaticamente nel file JSON in fase di distribuzione **Nota:** Questo campo può essere posizionato solo nell'oggetto modello.
categoria	Obbligatorio	String	Indica la modalità di popolamento del valore di ciascuna impostazione. É possibile selezionare uno dei seguenti valori: • **dynamic**. Il valore viene immesso dall'utente in fase di esecuzione. Lenovo XClarity Administrator richiede questo valore per la distribuzione del sistema operativo. • **predefined**. Il valore è preimpostato da Lenovo XClarity Administrator. • **static**. Il valore viene specificato nello schema e non cambia in fase di esecuzione. Gli oggetti nidificati ereditano il valore di questo campo dal relativo oggetto principale. Se **category** è impostato su `static` nell'oggetto principale, deve essere impostato su `static` anche in tutti gli oggetti nidificati. Se **category** è impostato su `dynamic` nell'oggetto principale, può essere `static` o `dynamic` negli oggetti nidificati.
scelte	opzionale	Array di valori che corrispondono alla proprietà **type**	Array di valori statici (come stringhe o numeri interi) per l'impostazione di configurazione che l'utente può selezionare durante la distribuzione del sistema operativo (ad esempio, `["enabled","disabled"]`).
comune	opzionale	Valore booleano	Indica se questo schema di configurazione si applica a tutti i server di destinazione. • **true**. L'oggetto si applica a tutti i server di destinazione. • **false**. (predefinito) L'oggetto si applica a un server di destinazione specifico. Gli oggetti nidificati ereditano il valore di questo campo dal relativo oggetto principale. Se **common** è impostato su `true` nell'oggetto principale, deve essere impostato su `true` anche in tutti gli oggetti nidificati. Se **common** è impostato su `false` nell'oggetto principale, deve essere impostato su `false` in tutti gli oggetti nidificati.

Parametro	Obbligatorio/ Facoltativo	Tipo	Descrizione
contenuto	opzionale	Matrice di oggetti	Pattern che rappresenta gli oggetti nidificati nello schema. Una volta raccolti i dati immessi dall'utente durante la distribuzione del sistema operativo, questo campo viene utilizzato per rappresentare i valori finali di un determinato modello nell'istanza del file delle impostazioni di configurazione creato per la distribuzione.
predefinito	opzionale	Varia a seconda del campo **tipo**	Il valore predefinito.
descrizione	opzionale	String	Descrizione dell'oggetto
etichetta	opzionale	String	Etichetta per l'impostazione nell'interfaccia utente visualizzata durante la distribuzione del sistema operativo
massimo	opzionale	Numero intero	Il valore massimo, quando **type** è impostato su un numero intero. Il valore predefinito è illimitato.
maxElements	opzionale	Numero intero	Numero massimo di voci nella matrice per questo oggetto.
min	opzionale	Numero intero	Il valore minimo, quando **type** è impostato su un numero intero. Il valore predefinito è 0.
minElements	opzionale	Numero intero	Numero minimo di voci nella matrice per questo oggetto.
name	Obbligatorio	String	Nome univoco dell'oggetto. Questo nome può contenere solo i seguenti caratteri: caratteri alfanumerici (a-z, A-Z e 0-9), carattere di sottolineatura (_) e trattino (-). È possibile fare riferimento al campo **name** come macro personalizzata nel file di installazione automatica. Quando si fa riferimento a un oggetto **name** nidificato, separare ogni oggetto utilizzando un punto (ad esempio, `mydeploy.node.locale`).
facoltativo	Obbligatorio	Valore booleano	Indica se l'oggetto è facoltativo. É possibile selezionare uno dei seguenti valori. • **true**. Il campo è facoltativo • **false**. Il campo è obbligatorio.
regex	opzionale	String	Espressione regolare per la convalida del valore (ad esempio, `"[\\w\\.]{1,64}$"`)
script	opzionale	Matrice di stringhe	Elenco di script, separati da una virgola, con dipendenze sui dati in questo oggetto (ad esempio, `["/opt/lenovo/saphana/bin/saphana-create-saphana.sh", "create_hana.sh"]`). **Nota:** Gli script devono essere disponibili nel profilo immagine del sistema operativo come script di installazione o software personalizzato.

Parametro	Obbligatorio/ Facoltativo	Tipo	Descrizione
targetServer	opzionale	String	L'UUID del server di destinazione per la distribuzione del sistema operativo. Se il parametro "common" è impostato su "true", questo campo può essere vuoto o NULL e il server di destinazione viene specificato durante la distribuzione del sistema operativo.

modello	opzionale	Matrice di oggetti	Pattern che rappresenta gli oggetti riutilizzabili.
			Durante la distribuzione del sistema operativo, questo modello può rappresentare più istanze dell'oggetto. I campi **minElements** e **maxElements** possono essere utilizzati per limitare il numero di istanze.
			
			Nel seguente esempio viene utilizzato un modello per rappresentare un array di 1-3 server NTP.
			`{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "NTP Servers",`
			`"label": "NTP Servers",`
			`"maxElements": 3,`
			`"minElements": 0,`
			`"name": "common-ntpservers",`
			`"optional": true,`
			`"template": [{`
			`"autoCreateInstance": true,`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "A NTP Server",`
			`"label": "NTP Server",`
			`"name": "ntpserver",`
			`"optional": true,`
			`"regex": "[\\w\\.]{1,64}$",`
			`"type": "string"`
			`}],`
			`"type": "array"`
			`},`
			
			Una volta raccolti i dati immessi dall'utente durante la distribuzione del sistema operativo, viene creata un'istanza del file delle impostazioni di configurazione con il contenuto specifico per ogni dispositivo su cui si desidera distribuire il sistema operativo.
			`{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "NTP Servers",`
			`"label": "NTP Servers",`
			`"maxElements": 3,`
			`"minElements": 0,`
			`"name": "common-ntpservers",`
			`"optional": true,`
			`"content": [{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "A NTP Server",`
			`"label": "NTP Server",`

Parametro	Obbligatorio/ Facoltativo	Tipo	Descrizione

			<pre>"name": "ntpserver0",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string",
			"value": "192.0.2.1"
			}],
			"template": [{
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			}</pre> **Nota:** • Un modello è *richiesto* nel livello superiore degli oggetti specifici del server (common=false). • Se **category** è impostato su `static`, il campo del modello viene ignorato.

tipo	Obbligatorio	String	Il tipo di dati per l'oggetto. É possibile selezionare uno dei seguenti valori. • **array** • **assoc_array** • **booleano** • **numero intero** • **password** • **stringa** • **user_data**
value	opzionale	String	Un singolo valore statico per l'impostazione di configurazione. **Nota:** • Se **default** è impostato, questo campo può essere vuoto o NULL; in caso contrario, specificare un valore che corrisponda al parametro **type**. • Se **type** è impostato su `password`, specificare una stringa non crittografata. • Se **type** è impostato su `assoc_array` o `array`, è necessario specificare anche un campo **content** vuoto. • Se **type** è impostato su `user_data`, specificare un parametro **value** valido in formato JSON. • Se **regex** è impostato, questo valore viene convalidato utilizzando l'espressione regolare specificata.

Le seguenti impostazioni di configurazione di esempio definiscono le impostazioni internazionali per le distribuzioni SLES che possono essere aggiunte a un profilo personalizzato.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "template": [{
            "autoCreateInstance": true,
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
                "type": "string",
                "value": "en_US"
            },
            {
                "category": "dynamic",
                "choices": ["english-us", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the keyboard locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "Keyboard Locale",
                "name": "keyboardLocale",
                "optional": false,
                "type": "string",
                "value": "english-us"
            }],
            "name": "server",
            "optional": false,
            "type": "assoc_array"
        }],
        "type": "assoc_array"
    },
    {
        "category": "dynamic",
        "common": true,
        "description": "NTP Servers",
        "label": "NTP Servers",
        "maxElements": 3,
        "minElements": 0,
        "name": "common-ntpservers",
        "optional": true,
        "template": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string"
        }],
        "type": "array"
```

```
    },
    {
        "category": "static",
        "common": true,
        "description": "Directory for post-installation script logging.",
        "name": "logpath",
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

Il seguente esempio rappresenta un'istanza del file delle impostazioni di configurazione creato sul sistema host, una volta definiti i valori immessi dall'utente durante la distribuzione.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "content": [{
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
                "type": "string",
                "value": "en_US"
            },
            {
                "category": "dynamic",
                "choices": ["english-us", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the keyboard locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "Keyboard Locale",
                "name": "keyboardLocale",
                "optional": false,
                "type": "string",
                "value": "english-us"
            }],
            "name": "server0",
            "optional": false,
            "type": "assoc_array",
            "targetServer": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
        },
        {
            "category": "dynamic",
```

```
    "common": false,
    "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the OS language locale to use with this deployment.
                        English, Brazilian Portuguese, and Japanese are supported.",
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
    },
    {
        "category": "dynamic",
        "choices": ["english-us", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the keyboard locale to use with this deployment.
                        English, Brazilian Portuguese, and Japanese are supported.",
        "label": "Keyboard Locale",
        "name": "keyboardLocale",
        "optional": false,
        "type": "string",
        "value": "english-us"
    }],
    "name": "server1",
    "optional": false,
    "type": "assoc_array",
    "targetServer": "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
}],
"template": [{
    "category": "dynamic",
    "common": false,
    "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the OS language locale to use with this deployment.
                        English, Brazilian Portuguese, and Japanese are supported.",
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
    },
    {
        "category": "dynamic",
        "choices": ["english-us", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the keyboard locale to use with this deployment.
                        English, Brazilian Portuguese, and Japanese are supported.",
        "label": "Keyboard Locale",
        "name": "keyboardLocale",
        "optional": false,
        "type": "string",
        "value": "english-us"
    }],
    "name": "server",
    "optional": false,
    "type": "assoc_array"
}],
```

```
        "type": "assoc_array"
    },
    {
        "category": "dynamic",
        "common": true,
        "description": "NTP Servers",
        "label": "NTP Servers",
        "maxElements": 3,
        "minElements": 0,
        "name": "common-ntpservers",
        "optional": true,
        "content": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver0,
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.1"
        },
        {
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver1",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.2"
        }],
        "template": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string"
        }],
        "type": "array"
    },
    {
        "category": "static",
        "common": true,
        "description": "Directory for post-installation script logs.",
        "name": "logpath",
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

Macro predefinite

Le *macro* forniscono la possibilità di aggiungere dati variabili (impostazioni di configurazione) a un file di installazione automatica o a uno script post-installazione. Lenovo XClarity Administrator include una serie di impostazioni di configurazione predefinite.

Per inserire macro predefinite in un file di installazione automatica o in uno script post-installazione, utilizzare il prefisso "predefinito" per le macro predefinite, separare gli oggetti nidificati con un punto e quindi racchiudere il nome della macro con il simbolo hash (#), ad esempio **#predefined.globalSettings.ipAssignment#**.

Il valore per ogni macro predefinita varia in base all'istanza di XClarity Administrator. Ad esempio, il campo **Distribuisci immagini sistema operativo → Impostazioni globali → Assegnazione IP** consente di specificare la modalità IP. Una volta raccolti i dati immessi dall'utente durante la distribuzione del sistema operativo, il valore viene rappresentato nelle impostazioni delle configurazioni predefinite dalla macro predefinita **#predefined.globalSettings.ipAssignment#** e nell'istanza di file JSON delle impostazioni di configurazione, denominato ipAssignment Object.

La seguente tabella elenca le macro predefinite (impostazioni di configurazione) disponibili in XClarity Administrator.

Nome macro	Tipo	Descrizione
predefinito	Object	Informazioni su tutte le impostazioni predefinite di distribuzione del sistema operativo
globalSettings	Object	Informazioni sulle impostazioni globali di distribuzione del sistema operativo
credenziali	Matrice di oggetti	Informazioni sulle credenziali utente
name	String	
tipo	String	Tipo di sistema operativo. É possibile selezionare uno dei seguenti valori. • **ESXi** • **LINUX** • **WINDOWS**
ipAssignment	String	L'opzione delle impostazioni di rete dell'host per la distribuzione del sistema operativo. É possibile selezionare uno dei seguenti valori. • **dhcpv4** • **staticv4** • **staticv6**
isVLANMode	String	Indica se viene utilizzata la modalità VLAN. É possibile selezionare uno dei seguenti valori. • **true**. La modalità VLAN viene utilizzata. • **false**. La modalità VLAN non viene utilizzata.
hostPlatforms	Object	Le impostazioni di distribuzione dalle piattaforme host
licenseKey	String	La chiave di licenza da utilizzare per Microsoft Windows o VMware ESXi. Se non si dispone di una chiave di licenza, è possibile lasciare vuoto questo campo.
networkSettings	Array	Informazioni sulle impostazioni di rete
dns1	String	Il server DNS preferito per il server host da utilizzare dopo la distribuzione del sistema operativo

Nome macro	Tipo	Descrizione
dns2	String	Il server DNS alternativo per il server host da utilizzare dopo la distribuzione del sistema operativo
gateway	String	Il gateway del server host da utilizzare dopo la distribuzione del sistema operativo. Viene utilizzato quando l'impostazione di rete è configurata su "statico" nelle impostazioni globali di distribuzione del sistema operativo. **Suggerimento:** per determinare la modalità IP, utilizzare GET /osdeployment/globalSettings.
Nome host	String	Il nome host per il server host. Se non viene specificato un nome host, viene assegnato un nome host predefinito.
ipAddress	String	L'indirizzo IP del server host da utilizzare dopo la distribuzione del sistema operativo. Viene utilizzato quando l'impostazione di rete è configurata su "statico" nelle impostazioni globali di distribuzione del sistema operativo.
mtu	Long	L'unità di trasmissione massima per l'host da utilizzare dopo la distribuzione del sistema operativo.
prefixLength	String	La lunghezza del prefisso dell'indirizzo IP dell'host da utilizzare dopo la distribuzione del sistema operativo. Viene utilizzato quando l'impostazione di rete è configurata su "IPv6 statico" nelle impostazioni globali di distribuzione del sistema operativo.
selectedMAC	String	L'indirizzo MAC del server host a cui associare l'indirizzo IP. L'indirizzo MAC è impostato su AUTO per impostazione predefinita. Questa impostazione rileva automaticamente le porte Ethernet che possono essere configurate e utilizzate per la distribuzione. Il primo indirizzo MAC (porta) rilevato viene utilizzato per impostazione predefinita. Se viene rilevata la connettività su un indirizzo MAC differente, l'host XClarity Administrator viene riavviato automaticamente per utilizzare l'indirizzo MAC appena rilevato per la distribuzione e selectedMAC vengono impostati con il nuovo indirizzo MAC rilevato. La modalità VLAN è supportata solo per i server che dispongono di indirizzi MAC nell'inventario. Se AUTO è l'unico indirizzo MAC disponibile per un server, non è possibile utilizzare VLAN per distribuire i sistemi operativi in tale server. **Suggerimento:** per ottenere l'indirizzo MAC, utilizzare la proprietà di risposta **macaddress** in GET /hostPlatforms.
subnetCIDRNumber	Numero intero	Maschera di sottorete del server host da utilizzare dopo la distribuzione del sistema operativo, in formato CIDR (Classless Inter-Domain Routing). Viene utilizzato quando l'impostazione di rete è configurata su "statico" nelle impostazioni globali di distribuzione del sistema operativo. Il numero CIDR è generalmente preceduto da una barra "/" e segue l'indirizzo IP. Ad esempio, un indirizzo IP 131.10.55.70 con una maschera di sottorete 255.0.0.0 (con 8 bit di rete) verrebbe rappresentato come 131.10.55.70 /8. Per ulteriori informazioni, consultare la sezione Pagina Web del tutorial sulla notazione CIDR. **Suggerimento:** per determinare la modalità IP, utilizzare GET /osdeployment/globalSettings.

Nome macro	Tipo	Descrizione
subnetMask	String	La maschera di sottorete del server host da utilizzare dopo la distribuzione del sistema operativo, in notazione decimale puntata (ad esempio, 255.0.0.0). Viene utilizzato quando l'impostazione di rete è configurata su "statico" nelle impostazioni globali di distribuzione del sistema operativo. **Suggerimento:** per determinare la modalità IP, utilizzare GET /osdeployment/globalSettings.
vlanId	String	L'ID VLAN per l'etichettatura VLAN del sistema operativo. Questo parametro è valido solo se la modalità VLAN è abilitata. Per determinare se la modalità VLAN è abilitata, utilizzare GET /osdeployment/globalSettings nella documentazione online di XClarity Administrator). **Importante:** Specificare un ID VLAN soltanto quando è necessaria un'etichetta VLAN per il funzionamento sulla rete. L'utilizzo di etichette VLAN può incidere sull'instradabilità della rete tra il sistema operativo host e XClarity Administrator.
selectedImage	String	L'ID del profilo dell'immagine del sistema operativo da distribuire. **Suggerimento:** per ottenere gli ID dei profili dell'immagine del sistema operativo, utilizzare la proprietà di risposta **availableImages** in GET /hostPlatforms.
storageSettings	Array	La posizione di storage preferita in cui si desidera distribuire le immagini del sistema operativo
targetDevice	String	Dispositivo di destinazione. É possibile selezionare uno dei seguenti valori. • **localdisk**. Unità disco locale. Viene utilizzata la prima unità disco locale enumerata del server gestito. • **Unità M.2**. Unità M.2. Viene utilizzata la prima unità M.2 enumerata del server gestito. • **usbdisk**. Hypervisor USB integrato. Questa posizione è applicabile solo se è in corso la distribuzione di un'immagine VMware ESXi sui server gestiti. Se sul server gestito sono installate due chiavi hypervisor, il programma di installazione VMware seleziona la prima chiave enumerata per la distribuzione. • **lunpluswwn=***LUN@WWN*. FC Storage SAN (ad esempio, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. Storage SAN iSCSI (ad esempio, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). L'opzione *IQN* è facoltativa se viene configurata una sola destinazione iSCSI. Se l'opzione *IQN* non viene specificata, viene selezionata la prima destinazione iSCSI rilevata per OSDN. Se invece l'opzione viene specificata, viene eseguita la corrispondenza esatta. **Nota:** Per i server ThinkServer, questo valore è sempre "localdisk."
unattendFileId	String	L'ID del file di installazione automatica da utilizzare con questa distribuzione
UUID	String	L'UUID del server host su cui distribuire il sistema operativo.
imageSettings	Object	Informazioni su ciascun immagine del sistema operativo e profilo immagine
name	String	Nome immagine del sistema operativo
profilo	String	Nome del profilo immagine
otherSettings	Object	Impostazioni aggiuntive correlate ai processi di distribuzione del sistema operativo attualmente in esecuzione

Nome macro	Tipo	Descrizione
deployDataAndSoftwareLocation	String	Il percorso del payload software estratto, dei file personalizzati e dei dati di distribuzione (come certificati e log)
installRepoUrl	String	URL (SLES 15 e solo versioni successive) per l'immagine del pacchetto importato È possibile utilizzare questa macro predefinita nel file di installazione automatica personalizzato per media_url nella sezione dei componenti aggiuntivi, ad esempio: <add-on> <add_on_products config:type="list"> <listentry> <media_url>**#predefined.otherSettings.installRepoUrl#** </media_url> <product>sle-module-basesystem</product> <product_dir>/Module-Basesystem</product_dir> </listentry> </add_on_products> </add-on>
lxcaIp	String	L'indirizzo IP dell'istanza XClarity Administrator
lxcaRelease	String	La versione di XClarity Administrator (ad esempio. 2.0.0)
jobId	String	L'ID del processo di distribuzione del sistema operativo attualmente in esecuzione
ntpServer	String	Il server NTP associato a XClarity Administrator
statusSettings	Object	Le impostazioni di stato per la distribuzione del sistema operativo
urlStatus	String	L'URL HTTPS (inclusa la porta) che XClarity Administrator utilizza per riportare lo stato
certLocation	String	Cartella contenente i certificati necessari per accedere al servizio Web **urlStatus** dall'host del sistema operativo al primo avvio
sdkLocation	String	La posizione di XClarity Administrator che ha fornito le interfacce e gli script helper per accedere a XClarity Administrator
timezone	String	Il fuso orario impostato per XClarity Administrator (ad esempio, America/New_York)
unattendSettings	Object	Le impostazioni utilizzate per popolare il file di installazione automatica. Questi valori sono specifici per la versione di XClarity Administrator
networkConfig	String	(Solo ESXi e RHEL) Il contenuto predefinito di XClarity Administrator da utilizzare nella fase di installazione automatica. Consente di configurare le impostazioni di rete per il sistema operativo
preinstallConfig	String	Il contenuto predefinito di XClarity Administrator da utilizzare nella fase di preinstallazione automatica. Include lo stato di preinstallazione. • Per ESXi e RHEL viene utilizzato l'hook degli script di preinstallazione %pre. • Per SLES, viene utilizzato l'hook degli script di preinstallazione <scripts>. **Attenzione:** Si consiglia di includere questa macro nel file di installazione automatica personalizzato. È possibile posizionare la macro nel file di installazione automatica dopo la riga 1 (dopo il tag <xml>).

Nome macro	Tipo	Descrizione
postinstallConfig	String	Il contenuto predefinito di XClarity Administrator da utilizzare una volta configurato e avviato il server per la prima volta. Includono lo stato di post-installazione. • Per ESXi e RHEL viene utilizzato l'hook degli script di post-installazione %post. • Per SLES, viene utilizzato l'hook degli script di post-installazione <scripts>. • Per Windows, viene utilizzata la sezione "impostazioni specializzate". **Attenzione:** Si consiglia di includere questa macro nel file di installazione automatica personalizzato. È possibile posizionare la macro nel file di installazione automatica dopo la riga 1 (dopo il tag <xml>).
reportWorkloadNotComplete	String	Quando è presente questa macro, la macro postinstallConfig non riporta lo stato Installazione del sistema operativo completata (17). Il profilo personalizzato deve essere indicato come completo.
storageConfig	String	(Solo ESXi e RHEL) Il contenuto predefinito di XClarity Administrator da utilizzare nella fase di installazione automatica. Consente di configurare le impostazioni di storage per il sistema operativo.

Importazione di file di installazione automatica personalizzati

È possibile importare file di installazione automatica personalizzati nel repository di immagini del sistema operativo. Questi file possono quindi essere utilizzati per personalizzare i profili immagine dei sistemi operativi Linux e Windows.

Informazioni su questa attività

Sono supportati i seguenti tipi di file di installazione automatica personalizzati.

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
CentOS Linux	Non supportato	
Azure Stack HCI di Microsoft® Windows®	Non supportato	
Microsoft Windows Hyper-V Server	Non supportato	
Microsoft Windows Server	Installazione automatica (.xml)	Per ulteriori informazioni sui file di installazione automatica, vedere Pagina Web di riferimento per l'installazione automatica di Windows.

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	Per ulteriori informazioni sui file di installazione automatica, vedere Red Hat: pagina Web sull'automazione dell'installazione con Kickstart. Tenere presente quando segue quando si aggiungono le sezioni %pre, %post, %firstboot al file. • È possibile includere più sezioni %pre, %post, %firstboot al file di installazione automatica. In tal caso, prestare attenzione all'ordinamento delle sezioni. • Quando la macro consigliata **#predefined. unattendSettings.preinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge una sezione %pre prima di tutte le altre sezioni %pre nel file. • Quando la macro consigliata **#predefined. unattendSettings.postinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge le sezioni %post e %firstboot prima di tutte le altre sezioni % post e %firstboot nel file.
Rocky Linux	Kickstart (.cfg)	Per ulteriori informazioni sui file di installazione automatica, vedere Red Hat: pagina Web sull'automazione dell'installazione con Kickstart. Tenere presente quando segue quando si aggiungono le sezioni %pre, %post, %firstboot al file. • È possibile includere più sezioni %pre, %post, %firstboot al file di installazione automatica. In tal caso, prestare attenzione all'ordinamento delle sezioni. • Quando la macro consigliata **#predefined. unattendSettings.preinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge una sezione %pre prima di tutte le altre sezioni %pre nel file. • Quando la macro consigliata **#predefined. unattendSettings.postinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge le sezioni %post e %firstboot prima di tutte le altre sezioni % post e %firstboot nel file.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	Per ulteriori informazioni sui file di installazione automatica, vedere SUSE: pagina Web di AutoYaST.

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
Ubuntu	Non supportato	
VMware vSphere® Hypervisor (ESXi) con Lenovo Customization	Kickstart (.cfg)	Supportato solo per ESXi 6.0u3 e gli aggiornamenti più recenti, nonché per la versione 6.5 e successive. Per ulteriori informazioni sui file di installazione automatica, vedere VMware: installazione o aggiornamento degli host mediante una pagina Web degli script. Tenere presente quando segue quando si aggiungono le sezioni %pre, %post, %firstboot al file. • È possibile includere più sezioni %pre, %post, %firstboot al file di installazione automatica. In tal caso, prestare attenzione all'ordinamento delle sezioni. • Quando la macro consigliata **#predefined.unattendSettings.preinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge una sezione %pre prima di tutte le altre sezioni %pre nel file. • Quando la macro consigliata **#predefined.unattendSettings.postinstallConfig#** è presente nel file di installazione automatica, XClarity Administrator aggiunge le sezioni %post e %firstboot prima di tutte le altre sezioni %post e %firstboot nel file.

Attenzione:

- È possibile inserire macro predefinite e personalizzate (impostazioni di configurazione) nel file di installazione automatica utilizzando il nome univoco dell'oggetto. I valori predefiniti sono dinamici in base alle istanze XClarity Administrator. Le macro personalizzate sono dinamiche in base all'input dell'utente, specificato durante la distribuzione del sistema operativo.

  Nota:

  - Racchiudere il nome della macro con il simbolo hash (#).
  - Per gli oggetti nidificati, separare ogni nome dell'oggetto con un punto (ad esempio, **#server_settings.server0.locale#**).
  - Per le macro personalizzate, non includere il nome dell'oggetto principale. Per le macro predefinite, utilizzare un prefisso "predefinito" per il nome della macro.
  - Quando viene creato un oggetto da un modello, il nome viene aggiunto con un numero univoco, a partire da 0 (ad esempio, **server0** e **server1**).
  - È possibile visualizzare il nome per ogni macro dalla finestra di dialogo Distribuisci immagini sistema operativo sulle schede Impostazioni personalizzate, passando il mouse sull'icona Guida ( ) accanto a ciascuna impostazione personalizzata.
  - Per un elenco di macro predefinite, vedere Macro predefinite. Per informazioni sulle impostazioni di configurazione personalizzate e le macro, vedere Macro personalizzate.
- XClarity Administrator fornisce le seguenti macro predefinite utilizzate per comunicare lo stato dal programma di installazione del sistema operativo, nonché altre diverse fasi di installazione critiche. Si consiglia di includere queste macro nel file di installazione automatica (vedere Inserimento di macro predefinite e personalizzate in un file di installazione automatica).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

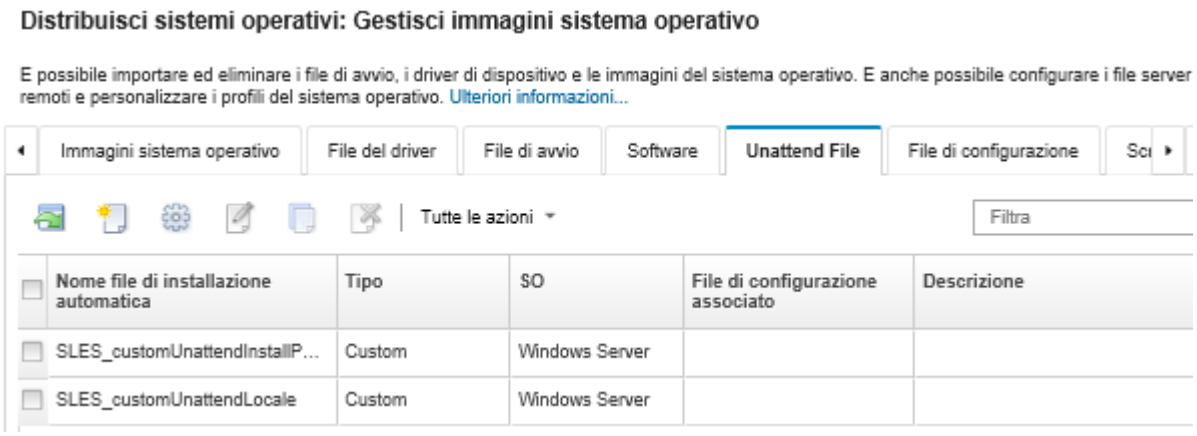
Il repository di immagini del sistema operativo consente di memorizzare un numero illimitato di file predefiniti e personalizzati, se è disponibile lo spazio per l'archiviazione dei file.

Procedura

Per importare i file di installazione automatica nel repository di immagini del sistema operativo, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.

Passo 2. Fare clic sulla scheda **File di installazione automatica**.



Passo 3. Fare clic sull'icona **Importa file** ( ). Viene visualizzata la finestra di dialogo "Importa file".

Passo 4. Fare clic sulla scheda **Importazione locale** per caricare i file dal sistema locale oppure fare clic sulla scheda **Importazione remota** per scaricare i file da un file server remoto.

Nota: Per caricare un file da un file server remoto, è necessario prima creare un profilo del file server remoto, facendo clic sull'icona **Configura file server** ( ). Per ulteriori informazioni, vedere Configurazione di un file server remoto .

Passo 5. Se si sceglie di utilizzare un file server remoto, selezionare il server che si desidera utilizzare dall'elenco **File server remoto**.

Passo 6. Selezionare il tipo di sistema operativo.

Passo 7. Immettere il nome del file di installazione automatica oppure fare clic su **Sfoglia** per individuare il file che si desidera importare.

Passo 8. **Facoltativo:** immettere una descrizione per il file di installazione automatica.

Suggerimento: utilizzare il campo **Descrizione** per distinguere i file personalizzati con lo stesso nome.

Passo 9. **Facoltativo:** selezionare un tipo di checksum per verificare che il file caricato non sia danneggiato e copiare e incollare il valore di checksum nel campo di testo fornito.

Se si seleziona un tipo di checksum, è necessario specificare un valore di checksum per controllare l'integrità e la sicurezza del file caricato. Il valore deve provenire da una un'origine sicura, da un'organizzazione attendibile. Se il file caricato corrisponde al valore di checksum, la distribuzione può essere eseguita in modo sicuro. In caso contrario, è necessario caricare nuovamente il file oppure controllare il valore di checksum.

Sono supportati tre tipi di checksum:

- **MD5**
- **SHA1**
- **SHA256**

Passo 10. Fare clic su **Importa**.

Suggerimento: il file viene caricato tramite una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione del file.

Se si chiude la scheda o la finestra del browser Web in cui il file viene caricato localmente prima del completamento dell'operazione, l'importazione non riesce.

Al termine

L'immagine del file di installazione automatica viene elencato nella scheda **File di installazione automatica** nella pagina Gestisci immagini sistema operativo.

Da questa pagina, è possibile completare le seguenti azioni.

- Creare un file di installazione automatica facendo clic sull'icona **Crea** ( ).

  L'editor identifica la posizione di eventuali errori rilevati nel file. Tenere presente che alcuni messaggi sono solo in inglese.
- Associare un file di installazione automatica a un file delle impostazioni di configurazione (vedere Associazione di un file di installazione automatica con un file delle impostazioni di configurazione).
- Visualizzare e modificare un file di installazione automatica facendo clic sull'icona **Modifica** ( ).

  L'editor identifica la posizione di eventuali errori rilevati nel file. Tenere presente che alcuni messaggi sono solo in inglese.
- Copiare un file di installazione automatica facendo clic sull'icona **Copia** ( ).

  Se si copia un file di installazione automatica associato a un file delle impostazioni di configurazione, viene copiato anche il file delle impostazioni di configurazione associato e l'associazione tra i due file copiati viene creata automaticamente.
- Rimuovere i file di installazione automatica selezionati facendo clic sull'icona **Elimina** ( ).
- Creare un profilo file server remoto, facendo clic sull'icona **Configura file server** ( ).

Per informazioni su come aggiungere un file di installazione automatica a un profilo immagine del sistema operativo personalizzato, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

Inserimento di macro predefinite e personalizzate in un file di installazione automatica

È possibile aggiungere macro predefinite e personalizzate a un file di installazione automatica.

Informazioni su questa attività

Le *macro* offrono la possibilità di aggiungere dati dinamici (impostazioni di configurazione) a un file di installazione automatica. Una volta distribuito il profilo immagine del sistema operativo è possibile fornire i valori dei dati.

Lenovo XClarity Administrator fornisce una serie di macro *predefinite* che è possibile aggiungere a un file di installazione automatica senza associare un file delle impostazioni di configurazione personalizzate. Per un elenco di macro predefinite, vedere Macro predefinite.

Si consiglia di includere le seguenti macro predefinite nei file di installazione automatica personalizzati.

- **#predefined.unattendSettings.preinstallConfig#** e **#predefined.unattendSettings postinstallConfig#**. Utilizzati per comunicare lo stato dal programma di installazione del sistema operativo, nonché altre diverse fasi di installazione critiche.

  Consultare i seguenti scenari di esempio di distribuzione del sistema operativo per ulteriori informazioni su come includere le macro di configurazione dell'installazione.
  - Distribuzione di RHEL e di un'applicazione Hello World PHP mediante un file di installazione automatica personalizzato
  - Distribuzione di SLES 12 SP3 con i server NTP e le impostazioni locali configurabili
  - Distribuzione di VMware ESXi v6.7 con Lenovo Customization su un disco locale utilizzando un indirizzo IP statico
  - Distribuzione di Windows 2016 con funzioni personalizzate
- **#predefined.unattendSettings.networkConfig#**. (Solo per ESXi e RHEL) Abilita XClarity Administrator a configurare la rete. Questa macro utilizza le impostazioni di rete specificate nella pagina Distribuisci immagini sistema operativo. Se non si include questa macro nel file di installazione automatica o se le impostazioni di rete non sono definite in XClarity Administrator è necessario configurare l'interfaccia IP nel file di installazione automatica, in modo che l'host disponga dell'instradamento di rete a XClarity Administrator.

  Consultare i seguenti scenari di esempio di distribuzione del sistema operativo per ulteriori informazioni su come includere la macro di configurazione della rete.
  - Distribuzione di RHEL e di un'applicazione Hello World PHP mediante un file di installazione automatica personalizzato
  - Distribuzione di VMware ESXi v6.7 con Lenovo Customization su un disco locale utilizzando un indirizzo IP statico
- **#predefined.unattendSettings.storageConfig#**. (Solo per ESXi e RHEL) Abilita XClarity Administrator a configurare lo storage sull'host. Questa macro utilizza le impostazioni di storage specificate nella pagina Distribuisci immagini sistema operativo. Se non si include questa macro nel file di installazione automatica o se le impostazioni di storage non sono definite in XClarity Administrator, è necessario specificare la configurazione di storage nel file di installazione automatica.

  Consultare i seguenti scenari di esempio di distribuzione del sistema operativo per ulteriori informazioni su come includere la macro di configurazione dello storage.
  - Distribuzione di RHEL e di un'applicazione Hello World PHP mediante un file di installazione automatica personalizzato
  - Distribuzione di VMware ESXi v6.7 con Lenovo Customization su un disco locale utilizzando un indirizzo IP statico

È possibile creare macro *personalizzate*, creando un file delle impostazioni di configurazione e quindi associando il file di installazione automatica a un file delle impostazioni di configurazione personalizzate. Quando si importa il file delle impostazioni di configurazione personalizzate, XClarity Administrator crea una macro per ogni impostazione di configurazione nel file.

Procedura

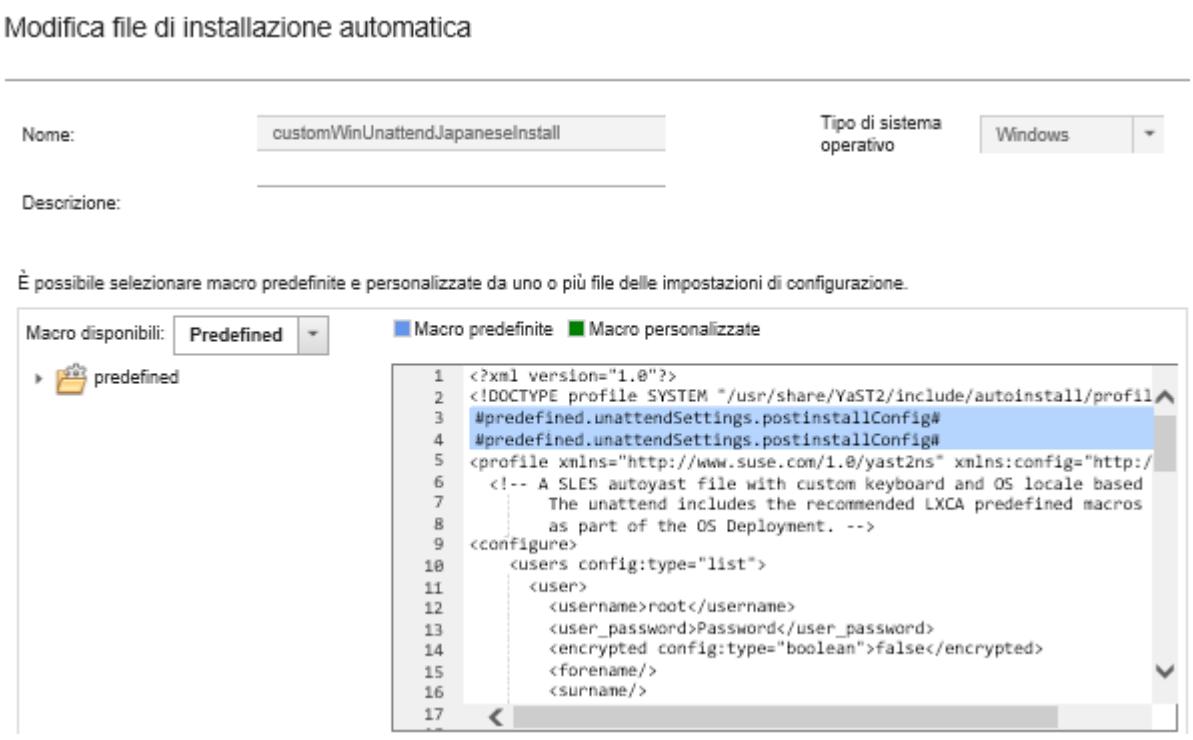
Completare le seguenti operazioni per aggiungere macro a un file di installazione automatica.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.

Passo 2. Fare clic sulla scheda **File di installazione automatica**.

Passo 3. Selezionare il file di installazione automatica che si desidera modificare.

Passo 4. Fare clic sull'icona **Modifica** ( ) per visualizzare la finestra di dialogo Modifica file di installazione automatica.



Passo 5. Aggiungere le macro predefinite consigliate, ad esempio:

1. Posizionare il cursore in un punto qualsiasi del file di installazione automatica dopo la riga 1 (dopo il tag <xml>).
2. Espandere l'elenco **predefinito → unattendSettings** nell'elenco di macro disponibili.
3. Fare clic su **preinstallConfig** e **postinstallConfig** per aggiungere le macro predefinite richieste al file di installazione automatica.

   Il seguente codice viene aggiunto al file:

   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#

Passo 6. Aggiungere macro predefinite o personalizzate aggiuntive posizionando il cursore nella posizione corretta del file di installazione automatica e facendo clic sulla macro dall'elenco.

Passo 7. Fare clic su **Salva**.

Associazione di un file di installazione automatica con un file delle impostazioni di configurazione

È possibile associare (collegare) le impostazioni di configurazione a un file di installazione automatica e quindi aggiungere le macro personalizzate associate al file di installazione automatica.

Informazioni su questa attività

È possibile aggiungere macro predefinite a un file di installazione automatica senza associare un file delle impostazioni di configurazione personalizzate.

Non è possibile modificare i file delle impostazioni di configurazione associati ai file di installazione automatica. Tuttavia, è possibile copiare un file associato e quindi modificare la copia.

Procedura

Completare le seguenti operazioni per associare un file di installazione automatica a un file delle impostazioni di configurazione.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.

Passo 2. Fare clic sulla scheda **File di installazione automatica**.

Passo 3. Selezionare il file di installazione personalizzato.

Passo 4. Fare clic sull'icona **Associa un file di configurazione** () per visualizzare la finestra di dialogo "Associa file di installazione automatica".

Passo 5. Selezionare un file delle impostazioni di configurazione da associare al file di installazione automatica.

Passo 6. Aggiungere le macro predefinite e personalizzate al file di installazione automatica, posizionando il cursore nella posizione dell'editor in cui si desidera aggiungere la macro e quindi fare clic sulla macro nell'elenco disponibile (vedere Inserimento di macro predefinite e personalizzate in un file di installazione automatica).

È possibile inserire macro nel file di installazione automatica utilizzando il nome univoco dell'oggetto. Per gli oggetti con nomi nidificati, separare ogni oggetto utilizzando un punto (ad esempio, `server_specific_settings.server.locale`). Accertarsi di non includere il nome principale.

Passo 7. Fare clic su **Associa** per associare i file.

Importazione di script di installazione personalizzati

È possibile importare gli script di installazione nel repository di immagini del sistema operativo. Questi file possono quindi essere utilizzati per personalizzare le immagini di Linux e Windows.

Informazioni su questa attività

Attualmente, sono supportati solo gli script post-installazione.

La seguente tabella elenca i tipi di file per gli script di installazione che Lenovo XClarity Administrator supporta per ciascun sistema operativo. Tenere presente che alcune versioni di sistema operativo non supportano tutti i tipi di file che XClarity Administrator supporta (ad esempio, alcune versioni di RHEL potrebbero non includere Perl nel profilo minimi e pertanto gli script Perl non verranno eseguiti). Accertarsi di utilizzare il tipo di file corretto per le versioni del sistema operativo che si desidera distribuire.

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
CentOS Linux	Non supportato	
Azure Stack HCI di Microsoft® Windows®	Non supportato	
Microsoft Windows Hyper-V Server	Non supportato	
Microsoft® Windows® Server	File di comando (.cmd), PowerShell (.ps1)	Il percorso predefinito di file e dati personalizzati è `C:\lxca`. Per ulteriori informazioni sugli script di installazione, vedere Pagina Web sull'aggiunta di uno script personalizzato all'installazione di Windows

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm o .pl), Python (.py)	Il percorso predefinito di file e dati personalizzati è `/home/lxca`. Per ulteriori informazioni sugli script di installazione, vedere RHEL: pagina Web degli script post-installazione.
Rocky Linux	Bash (.sh), Perl (.pm o .pl), Python (.py)	Il percorso predefinito di file e dati personalizzati è `/home/lxca`. Per ulteriori informazioni sugli script di installazione, vedere RHEL: pagina Web degli script post-installazione
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm o .pl), Python (.py)	Il percorso predefinito di file e dati personalizzati è `/home/lxca`. Per ulteriori informazioni sugli script di installazione, vedere SUSE: pagina Web degli script utente personalizzati
Ubuntu	Non supportato	
VMware vSphere® Hypervisor (ESXi) con Lenovo Customization	Bash (.sh), Python (.py)	Il percorso predefinito di file e dati personalizzati è `/home/lxca`. Per ulteriori informazioni sugli script di installazione, vedere VMware: pagina Web degli script di aggiornamento e installazione

Nota: Il repository di immagini del sistema operativo consente di memorizzare un numero illimitato di file predefiniti e personalizzati, se è disponibile lo spazio per l'archiviazione dei file.

Una volta raccolti i dati durante la distribuzione del sistema operativo, XClarity Administrator crea un'istanza del file delle impostazioni di configurazione (che include le impostazioni personalizzate nel file selezionato e un sottoinsieme di impostazioni predefinite) sul sistema host, che può essere utilizzato dallo script post-installazione.

È possibile inserire macro predefinite e personalizzate (impostazioni di configurazione) nello script post-installazione utilizzando il nome univoco dell'oggetto. I valori predefiniti sono dinamici in base alle istanze XClarity Administrator. Le macro personalizzate sono dinamiche in base all'input dell'utente, specificato durante la distribuzione del sistema operativo.

Nota:

- Racchiudere il nome della macro con il simbolo hash (#).
- Per gli oggetti nidificati, separare ogni nome dell'oggetto con un punto (ad esempio, **#server_settings.server0.locale#**).
- Per le macro personalizzate, non includere il nome dell'oggetto principale. Per le macro predefinite, utilizzare un prefisso "predefinito" per il nome della macro.
- Quando viene creato un oggetto da un modello, il nome viene aggiunto con un numero univoco, a partire da 0 (ad esempio, **server0** e **server1**).
- È possibile visualizzare il nome per ogni macro dalla finestra di dialogo Distribuisci immagini sistema operativo sulle schede Impostazioni personalizzate, passando il mouse sull'icona Guida () accanto a ciascuna impostazione personalizzata.
- Per un elenco di macro predefinite, vedere Macro predefinite. Per informazioni sulle impostazioni di configurazione personalizzate e le macro, vedere Macro personalizzate.

Le macro predefinite consigliate nel file di installazione automatica riportano lo stato finale di distribuzione del sistema operativo e lo stato di download ed esecuzione degli script post-installazione. È possibile modificare lo script post-installazione per includere il report di stato personalizzato, a seconda del sistema operativo di destinazione. Per ulteriori informazioni, vedere Aggiunta di report di stato personalizzato agli script di installazione.

Procedura

Per importare gli script di installazione nel repository di immagini del sistema operativo, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.

Passo 2. Fare clic sulla scheda **Script di installazione**.

Passo 3. Fare clic sull'icona **Importa file** ( ). Verrà visualizzata la finestra di dialogo "Importa script di installazione".

Passo 4. Fare clic sulla scheda **Importazione locale** per caricare i file dal sistema locale oppure fare clic sulla scheda **Importazione remota** per scaricare i file da un file server remoto.

Nota: Per caricare un file da un file server remoto, è necessario prima creare un profilo del file server remoto, facendo clic sull'icona **Configura file server** ( ). Per ulteriori informazioni, vedere Configurazione di un file server remoto .

Passo 5. Se si sceglie di utilizzare un file server remoto, selezionare il server che si desidera utilizzare dall'elenco **File server remoto**.

Passo 6. Selezionare il tipo di sistema operativo.

Passo 7. Immettere il nome del file dello script di installazione oppure fare clic su **Sfoglia** per individuare il file che si desidera importare.

Passo 8. **Facoltativo:** immettere una descrizione per lo script di installazione.

Suggerimento: utilizzare il campo **Descrizione** per distinguere i file personalizzati con lo stesso nome.

Passo 9. **Facoltativo:** selezionare un tipo di checksum per verificare che il file caricato non sia danneggiato e copiare e incollare il valore di checksum nel campo di testo fornito.

Se si seleziona un tipo di checksum, è necessario specificare un valore di checksum per controllare l'integrità e la sicurezza del file caricato. Il valore deve provenire da una un'origine sicura, da un'organizzazione attendibile. Se il file caricato corrisponde al valore di checksum, la distribuzione può essere eseguita in modo sicuro. In caso contrario, è necessario caricare nuovamente il file oppure controllare il valore di checksum.

Sono supportati tre tipi di checksum:
- **MD5**
- **SHA1**
- **SHA256**

Passo 10. Fare clic su **Importa**.

Suggerimento: il file viene caricato tramite una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione del file.

Se si chiude la scheda o la finestra del browser Web in cui il file viene caricato localmente prima del completamento dell'operazione, l'importazione non riesce.

Al termine

Gli script di installazione sono elencati nella scheda **Script di installazione** nella pagina Gestisci immagini sistema operativo.

Da questa pagina, è possibile completare le seguenti azioni.

- Creare un profilo file server remoto, facendo clic sull'icona **Configura file server** ().
- Rimuovere gli script di installazione selezionati facendo clic sull'icona **Elimina** ().

Per informazioni su come aggiungere uno script di installazione a un profilo immagine del sistema operativo personalizzato, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

Aggiunta di report di stato personalizzato agli script di installazione

Le macro predefinite consigliate nel file di installazione automatica riportano lo stato finale di distribuzione del sistema operativo e lo stato di download ed esecuzione degli script post-installazione. È possibile includere report di stato aggiuntivi negli script post-installazione.

Linux

Per Linux, è possibile utilizzare il seguente comando `curl` per riportare lo stato.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"<status_ID>"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Dove <*status_ID*> può essere uno dei seguenti valori.
- **44**. Distribuzione del carico di lavoro riuscita
- **45**. Distribuzione del carico di lavoro in esecuzione con avvertenza
- **46**. Distribuzione del carico di lavoro non riuscita
- **47**. Messaggio di distribuzione del carico di lavoro
- **48**. Errore dello script post-installazione personalizzato

Tenere presente che il comando `curl` utilizza macro predefinite per l'URL HTTPS che Lenovo XClarity Administrator usa per segnalare lo stato (**predefined.otherSettings.statusSettings.urlStatus**) e per la cartella contenente i certificati necessari per accedere al servizio web urlStatus dal sistema operativo host al primo avvio (**predefined.otherSettings.statusSettings.certLocation**). Il seguente esempio riporta un errore che si è verificato nello script post-installazione.

Il seguente esempio riporta un errore che si è verificato nello script post-installazione.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"48"}}'
```

```
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Windows

Per Wiindows, è possibile importare lo script `LXCA.psm1` e quindi richiamare i seguenti comandi per segnalare lo stato.

- **initializeRestClient**

  Inizializza il client REST. Utilizzare la seguente sintassi per eseguire questo comando. Questo comando è richiesto prima di eseguire i comandi di report.

  ```
  initializeRestClient
  ```

- **testLXCAConnection**

  Verifica che XClarity Administrator può collegarsi al server host. Utilizzare la seguente sintassi per eseguire questo comando. Questo comando è facoltativo ma consigliato nello script di installazione prima di eseguire i comandi di report.

  ```
  testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"
  ```

- **reportWorkloadDeploymentSucceeded**

  Riporta un messaggio di completamento riuscito da aggiungere al log dei processi di XClarity Administrator. Utilizzare la seguente sintassi per eseguire questo comando.

  Suggerimento: se la macro **#predefined.unattendSettings.reportWorkloadNotComplete#** è inclusa in un file di installazione automatica personalizzato o nello script post-installazione, includere il comando **reportWorkloadDeploymentSucceeded** nello script post-installazione per indicare un completamento riuscito. In caso contrario, XClarity Administrator riporta automaticamente lo stato "Completo", dopo l'esecuzione di tutti gli script post-installazione.

  ```
  reportWorkloadDeploymentSucceeded -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#"
  ```

- **reportWorkloadDeploymentRunningWithWarning**

  Riporta un messaggio di avvertenza da registrare nel log dei processi di XClarity Administrator. Utilizzare la seguente sintassi per eseguire questo comando.

  ```
  reportWorkloadDeploymentRunningWithWarning -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" –WarningMessage "<message_text>"
  ```

- **reportWorkloadDeploymentFailed**

  Riporta un messaggio di errore da registrare nel log dei processi di XClarity Administrator. Utilizzare la seguente sintassi per eseguire questo comando.

  ```
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "<message_text>"
  ```

- **reportCustomPostInstallScriptError**

  Riporta un messaggio di errore dello script post-installazione da registrare nel log dei processi di XClarity Administrator. Utilizzare la seguente sintassi per eseguire questo comando.

  ```
  reportCustomPostInstallScriptError -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

- **reportWorkloadDeploymentMessage**

  Riporta un messaggio generale per da registrare nel log dei processi di XClarity Administrator senza compromettere lo stato della distribuzione. Utilizzare la seguente sintassi per eseguire questo comando.

  ```
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

Dove <*message_text*> è il messaggio che si desidera restituire a XClarity Administrator per ogni condizione di stato.

Tenere presente che questi comandi utilizzano macro predefinite per l'indirizzo IP dell'istanza di XClarity Administrator (**#predefined.otherSettings.lxcaIp#**) e per l'UUID del server host su cui verrà distribuito il sistema operativo (**#predefined.hostPlatforms.uuid#**).

Il seguente esempio è uno script post-installazione PowerShell che installa Java e segnala un errore, se l'installazione non riesce

```
import-module C:\windows\system32\WindowsPowerShell\v1.0\Modules\LXCA\LXCA.psm1

initializeRestClient

testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"

Write-Output "Reporting status to Lenovo XClarity Administator…"
   reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
   -UUID "#predefined.hostPlatforms.uuid#" -Message "Installing Java"

Write-Output "Install Java…."
   Invoke-Command -ScriptBlock {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
   [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg] /s}

if ($LastExitCode -ne 0) {
   reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
      -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "Java could not be installed"
}

Write-Output "Completed install of Java for Administrator user."
```

Importazione di software personalizzato

È possibile importare il software nel repository di immagini del sistema operativo. Questi file possono quindi essere utilizzati per personalizzare le immagini di Linux e Windows

Informazioni su questa attività

I file del software personalizzato vengono installati una volta completata la distribuzione del sistema operativo e degli script post-installazione.

Sono supportati i seguenti tipi di file per il software personalizzato.

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
CentOS Linux	Non supportato	
Azure Stack HCI di Microsoft® Windows®	Non supportato	
Microsoft Windows Hyper-V Server	Non supportato	
Microsoft Windows® Server	Un file .zip contenente il payload del software.	Il percorso predefinito di file e dati personalizzati è `C:\lxca`.
Red Hat® Enterprise Linux (RHEL) Server	Un file .tar.gz contenente il payload del software	Il percorso predefinito di file e dati personalizzati è `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	Un file .tar.gz contenente il payload del software	Il percorso predefinito di file e dati personalizzati è `/home/lxca`.

Sistema operativo	Tipi di file supportati	Ulteriori informazioni
Rocky Linux	Un file .tar.gz contenente il payload del software	Il percorso predefinito di file e dati personalizzati è `/home/lxca`.
Ubuntu	Non supportato	
VMware vSphere® Hypervisor (ESXi) con Lenovo Customization	Un file .tar.gz contenente il payload del software	Il percorso predefinito di file e dati personalizzati è `/home/lxca`.

Nota: Il repository di immagini del sistema operativo consente di memorizzare un numero illimitato di file predefiniti e personalizzati, se è disponibile lo spazio per l'archiviazione dei file.

Procedura

Per importare il software nel repository di immagini del sistema operativo, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.

Passo 2. Fare clic sulla scheda **Software**.

Passo 3. Fare clic sull'icona **Importa file** ( ). Verrà visualizzata la finestra di dialogo "Importa script di installazione".

Passo 4. Fare clic sulla scheda **Importazione locale** per caricare i file dal sistema locale oppure fare clic sulla scheda **Importazione remota** per scaricare i file da un file server remoto.

Nota: Per caricare un file da un file server remoto, è necessario prima creare un profilo del file server remoto, facendo clic sull'icona **Configura file server** ( ). Per ulteriori informazioni, vedere Configurazione di un file server remoto .

Passo 5. Se si sceglie di utilizzare un file server remoto, selezionare il server che si desidera utilizzare dall'elenco **File server remoto**.

Passo 6. Selezionare il tipo di sistema operativo.

Passo 7. Immettere il nome file del software oppure fare clic su **Sfoglia** per individuare il file che si desidera importare.

Passo 8. **Facoltativo:** immettere una descrizione del file del software.

Suggerimento: utilizzare il campo **Descrizione** per distinguere i file personalizzati con lo stesso nome.

Passo 9. **Facoltativo:** selezionare un tipo di checksum per verificare che il file caricato non sia danneggiato e copiare e incollare il valore di checksum nel campo di testo fornito.

Se si seleziona un tipo di checksum, è necessario specificare un valore di checksum per controllare l'integrità e la sicurezza del file caricato. Il valore deve provenire da una un'origine sicura, da un'organizzazione attendibile. Se il file caricato corrisponde al valore di checksum, la distribuzione può essere eseguita in modo sicuro. In caso contrario, è necessario caricare nuovamente il file oppure controllare il valore di checksum.

Sono supportati tre tipi di checksum:
- **MD5**
- **SHA1**
- **SHA256**

Passo 10. Fare clic su **Importa**.

Suggerimento: il file viene caricato tramite una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione del file.

Se si chiude la scheda o la finestra del browser Web in cui il file viene caricato localmente prima del completamento dell'operazione, l'importazione non riesce.

Al termine

Gli script di installazione sono elencati nella scheda **Software** nella pagina Gestisci immagini sistema operativo.

Da questa pagina, è possibile completare le seguenti azioni.

- Creare un profilo file server remoto, facendo clic sull'icona **Configura file server** ( ).
- Rimuovere i file del software selezionati facendo clic sull'icona **Elimina** ( ).

Per informazioni su come aggiungere un file del software a un profilo immagine del sistema operativo personalizzato, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

Creazione di un profilo immagine del sistema operativo personalizzato

È possibile aggiungere i driver di dispositivo personalizzati, i file di avvio (solo Windows), le impostazioni di configurazione, i file di installazione automatica, gli script di installazione e il software a un profilo immagine del sistema operativo predefinito, presente nel repository di immagini del sistema operativo. Quando si aggiungono dei file a un'immagine del sistema operativo, Lenovo XClarity Administrator crea un profilo personalizzato di immagine del sistema operativo per tale immagine. Il profilo personalizzato include i file personalizzati e le opzioni di installazione.

Prima di iniziare

I file personalizzati da aggiungere devono esistere nel repository delle immagini del sistema operativo (vedere Importazione dei file di avvio, Importazione dei driver di dispositivo, Importazione delle impostazioni di configurazione personalizzate, Importazione di file di installazione automatica personalizzati, Importazione di script di installazione personalizzati e Importazione di software personalizzato).

Procedura

Per personalizzare un'immagine del sistema operativo, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.

Passo 2. Fare clic sulla scheda **Immagini sistema operativo**.

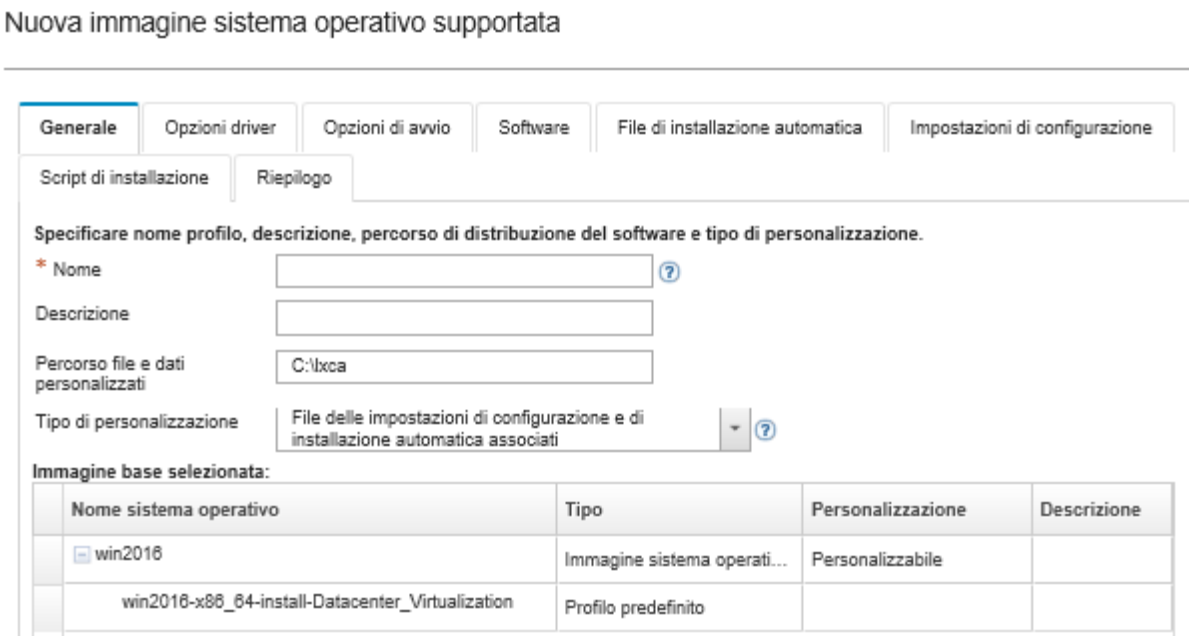
Passo 3. Selezionare il profilo predefinito dell'immagine del sistema operativo che si desidera personalizzare.

La colonna **Personalizzazione** identifica le immagini del sistema operativo che possono essere personalizzate. Per ulteriori informazioni sulla personalizzazione di un'immagine specifica del sistema operativo, fare clic sull'icona **Guida** ( ).

- **Personalizzabile**. L'immagine del sistema operativo supporta la personalizzazione ma non è personalizzata.
- **Non personalizzabile**. L'immagine del sistema operativo non supporta la personalizzazione.

Nota: È possibile importare immagini del sistema operativo di base aggiuntive (in formato .iso) da un sistema locale o remoto, facendo clic sull'icona **Importa file** ( ).

Passo 4. Fare clic sull'icona **Crea profilo personalizzato** ( ). Viene visualizzata la finestra di dialogo "Nuova immagine personalizzata sistema operativo".



Passo 5. Nella scheda **Generale** specificare nome, descrizione, percorso per i file personalizzati e i dati di distribuzione sull'host di distribuzione e il tipo di personalizzazione per il nuovo profilo immagine del sistema operativo personalizzato.

È possibile utilizzare uno dei seguenti tipi di personalizzazione:

- **Solo file di installazione automatica**
- **Solo file di configurazione**
- **File di configurazione e di installazione automatica non associati**
- **File di configurazione e di installazione automatica associati**
- **Nessuno**

Passo 6. Fare clic su **Avanti**.

Passo 7. Dalla scheda **Driver di dispositivo**, selezionare l'unità del dispositivo che si desidera aggiungere al profilo immagine del sistema operativo Linux.

Per un elenco dei formati supportati, vedere Importazione dei driver di dispositivo.

Il file selezionato viene applicato una volta completata la configurazione guidata.

Nota: È possibile importare driver di dispositivo aggiuntivi da un sistema locale o remoto, facendo clic sull'icona **Importa file** ().

Passo 8. Fare clic su **Avanti**.

Passo 9. (Solo Windows) Dalla scheda **Opzioni di avvio**, selezionare i file di avvio che si desidera aggiungere al profilo immagine del sistema operativo Windows.

Per un elecnco dei formati supportati, vedere Importazione dei file di avvio.

Il file selezionato viene applicato una volta completata la configurazione guidata.

Passo 10. Fare clic su **Avanti**.

Passo 11. Nella scheda **Impostazioni di configurazione** (se applicabile), selezionare uno o più file di configurazione personalizzati che si desidera aggiungere al profilo immagine del sistema operativo. È possibile selezionare massimo un file

Passo 12. Fare clic su **Avanti**.

Passo 13. Nella scheda **File di installazione automatica**:

a. Selezionare il file di installazione automatica che si desidera aggiungere al profilo immagine del sistema operativo.

   Per un elenco dei formati supportati, vedere Importazione di file di installazione automatica personalizzati.

   Il file selezionato viene applicato una volta completata la configurazione guidata.

b. Selezionare un file di configurazione da associare al file di installazione automatica dalla colonna **File di configurazione associati**

c. Facoltativamente, selezionare le macro personalizzate disponibili nel file di configurazione selezionato o aggiungere le macro personalizzate in formato. xml.

Passo 14. Fare clic su **Avanti**.

Passo 15. Dalla scheda **Script di installazione** (se applicabile), selezionare gli script di installazione che si desidera aggiungere al profilo immagine del sistema operativo Windows. È possibile selezionare massimo uno script post-installazione.

Per un elenco dei formati supportati, vedere Importazione di script di installazione personalizzati.

Il file selezionato viene applicato una volta completata la configurazione guidata.

Nota: È possibile importare script di installazione aggiuntivi da un sistema locale o remoto, facendo clic sull'icona **Importa file** ().

Passo 16. Fare clic su **Avanti**.

Passo 17. Dalla scheda **Software**, selezionare il software che si desidera aggiungere al profilo immagine del sistema operativo Linux.

Per un elenco dei formati supportati, vedere Importazione di software personalizzato.

Il file selezionato viene applicato una volta completata la configurazione guidata.

Nota: È possibile importare software aggiuntivi da un sistema locale o remoto, facendo clic sull'icona **Importa file** ().

Passo 18. Fare clic su **Avanti**.

Passo 19. Verificare le impostazioni nella scheda **Riepilogo** e fare clic su **Personalizza** per creare il profilo personalizzato di immagine del sistema operativo.

Al termine

Il profilo personalizzato di immagine del sistema operativo viene riportato nel sistema operativo di base nella scheda **Immagini sistema operativo** della pagina "Gestisci immagini sistema operativo".

Da questa pagina, è possibile eseguire le seguenti azioni:

- Importare un profilo personalizzato di immagine del sistema operativo e applicarlo a un'immagine del sistema operativo di base facendo clic su **Importa/Esporta profilo → Esporta immagine del profilo personalizzata** (vedere Importazione di un profilo immagine del sistema operativo personalizzato).
- Esportare un profilo immagine del sistema operativo personalizzato selezionato facendo clic su **Importa/esporta profilo → Esporta immagine del profilo personalizzato**.
- Modificare un profilo personalizzato di immagine del sistema operativo selezionato, facendo clic sull'icona **Modifica** ( ).
- Rimuovere un profilo personalizzato di immagine del sistema operativo selezionato, facendo clic sull'icona **Elimina** ( ).

Configurazione delle impostazioni globali di distribuzione del sistema operativo

Le impostazioni globali fungono da impostazioni di impostazioni predefinite quando vengono distribuiti i sistemi operativi.

Informazioni su questa attività

Nella pagina Impostazioni globali è possibile configurare le seguenti impostazioni:

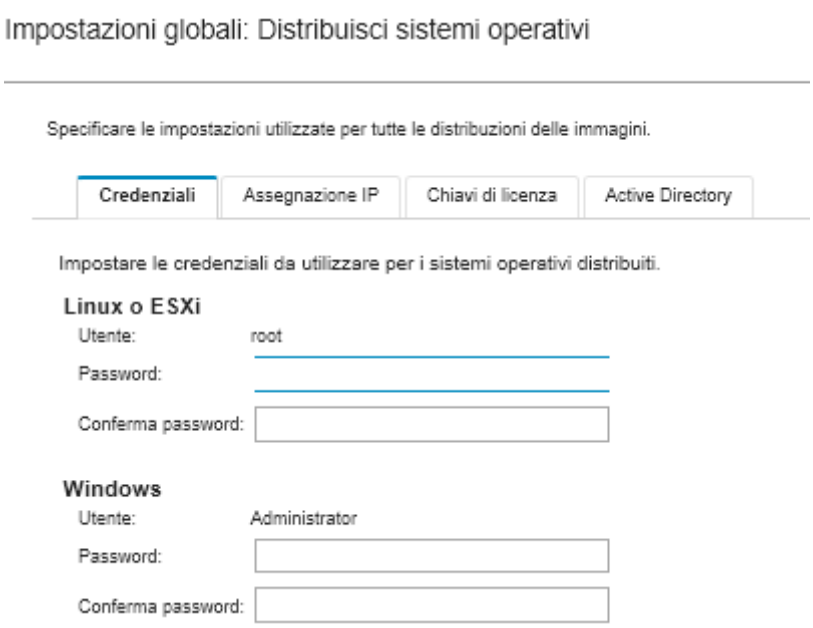
- La password per l'account utente dell'amministratore da utilizzare per distribuire i sistemi operativi
- Il metodo da utilizzare per assegnare gli indirizzi IP ai server
- I codici di licenza da utilizzare quando si attivano i sistemi operativi installati
- Facoltativamente, unire un dominio di Active Directory nell'ambito della distribuzione del sistema operativo Windows

Procedura

Per configurare le impostazioni globali da utilizzare per tutti i server, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci immagini sistema operativo.

Passo 2. Fare clic sull'icona **Impostazioni globali** ( ) per visualizzare la finestra di dialogo Impostazioni globali: distribuisci sistemi operativi.



Passo 3. Sulla scheda **Credenziali**, immettere la password che deve essere utilizzata dall'account dell'amministratore per eseguire il login al sistema operativo.

Passo 4. Sulla scheda **Assegnazione IP**, selezionare le seguenti opzioni.

a. **Facoltativo:** selezionare **Usa VLAN** per consentire la configurazione delle impostazioni VLAN nella finestra di dialogo Impostazioni di rete (vedere Configurazione delle impostazioni di rete per i server gestiti).

Nota: Note:

- L'etichettatura VLAN non è supportata per le distribuzioni dei sistemi operativi Linux.
- L'etichettatura VLAN non è supportata per le distribuzioni dei sistemi operativi sui dispositivi ThinkServer.
- La modalità VLAN è supportata solo per i server che dispongono di indirizzi MAC nell'inventario. Se AUTO è l'unico indirizzo MAC disponibile per un server, non è possibile utilizzare le VLAN per distribuire i sistemi operativi a tale server.

b. Selezionare il metodo per assegnare gli indirizzi IP quando si configura il sistema operativo distribuito:

Nota: Per collegare il controller di gestione della scheda di base è necessario configurare l'interfaccia di rete di XClarity Administrator utilizzata per la gestione, utilizzando lo stesso metodo dell'indirizzo IP selezionato nella finestra di dialogo Impostazioni globali: Distribuisci sistemi operativi. Ad esempio, se XClarity Administrator è configurato per utilizzare eth0 per la gestione e si sceglie di usare gli indirizzi IPv6 statici assegnati manualmente durante la configurazione del sistema operativo distribuito, eth0 deve essere configurato con un indirizzo IPv6 che disponga della connettività al controller di gestione della scheda di base.

- **Assegna manualmente un indirizzo IPv4 statico**. Se si decide di assegnare indirizzi IPv4 statici, assicurarsi di configurare l'indirizzo IPv4 statico, l'indirizzo gateway e la maschera di sottorete per il server prima di distribuire il sistema operativo (vedere Configurazione delle impostazioni di rete per i server gestiti).
- **Usa DHCP (Dynamic Host Configuration Protocol) per assegnare gli indirizzi** Se si dispone già di una infrastruttura DHCPv4 esistente nella rete, è possibile utilizzare tale infrastruttura per assegnare gli indirizzi IP ai server.

  Nota: L'indirizzo IPv6 DHCP non è supportato per la distribuzione dei sistemi operativi.

- **Assegna manualmente un indirizzo IPv6 statico**. Se si sceglie di assegnare indirizzi IPv6 statici, assicurarsi di configurare l'indirizzo IPv6 statico, l'indirizzo gateway e la maschera di sottorete per il server prima di distribuire il sistema operativo (vedere Configurazione delle impostazioni di rete per i server gestiti).

Passo 5. **Facoltativo:** sulla scheda **Chiavi di licenza**, specificare le chiavi di licenza dei volume globali da utilizzare quando si attivano i sistemi operativi Windows installati.

Quando si specificano le chiavi di licenza dei volumi globali su questa scheda, è possibile selezionare le chiavi di licenza specificate per tutti i profili di immagini del sistema operativo Windows dalla pagina Distribuisci immagini sistema operativo.

Suggerimento: XClarity Administrator supporta le chiavi di licenza dei volumi globali per le installazioni Windows e le singole chiavi di licenza retail per Windows e VMware ESXi. È possibile specificare le singole chiavi di vendita retail nell'ambito della procedura di distribuzione (vedere Distribuzione di un'immagine del sistema operativo).

Passo 6. **Facoltativo:** sulla scheda **Active Directory**, configurare le impostazioni di Active Directory per le distribuzioni del sistema operativo Windows. Per informazioni sull'integrazione con Active Directory, vedere Integrazione con Windows Active Directory.

Passo 7. Fare clic su **OK** per chiudere la finestra di dialogo.

Configurazione delle impostazioni di rete per i server gestiti

Le impostazioni di rete sono opzioni di configurazione specifiche di ciascun server. È necessario configurare le impostazioni di rete per un server gestito prima di poter distribuire un sistema operativo a tale server.

Informazioni su questa attività

Se si utilizza DHCP per assegnare dinamicamente gli indirizzi IP, è necessario configurare l'indirizzo MAC.

Se si utilizzano indirizzi IP statici, è necessario configurare le seguenti impostazioni di rete per un server specifico prima di poter distribuire un sistema operativo a tale server. Dopo aver configurato tali impostazioni, lo stato di distribuzione delle modifiche del server viene modificato in "Pronto". Alcuni campi non sono disponibili per gli indirizzi IPv6 statici.

- Nome host

  Il nome host deve essere conforme alle seguenti regole:
  - Il nome host di ciascun server gestito deve essere univoco.
  - Il nome host può contenere stringhe (etichette) separate da un punto (.).
  - Ogni etichetta può contenere lettere, numeri e trattini (-) ASCII; tuttavia, la stringa non può iniziare o terminare con un trattino e non può contenere solo numeri.
  - La prima etichetta può avere una lunghezza compresa tra 2 e 15 caratteri. Le etichette successive possono avere una lunghezza compresa tra 2 e 63 caratteri.
  - La lunghezza totale del nome host non deve superare i 255 caratteri.
- L'indirizzo MAC della porta sull'host in cui deve essere installato il sistema operativo.

  L'indirizzo MAC è impostato su AUTO per impostazione predefinita. Questa impostazione rileva automaticamente le porte Ethernet che possono essere configurate e utilizzate per la distribuzione. Il primo indirizzo MAC (porta) rilevato viene utilizzato per impostazione predefinita. Se viene rilevata la connettività su un indirizzo MAC differente, l'host XClarity Administrator viene riavviato automaticamente per utilizzare l'indirizzo MAC appena rilevato per la distribuzione.

  È possibile determinare lo stato della porta dell'indirizzo MAC utilizzata per la distribuzione del sistema operativo dal menu a discesa **Indirizzo MAC** nella finestra di dialogo Impostazioni di rete. Se sono presenti più porte o se tutte le porte sono disattivate, viene utilizzato AUTO per impostazione predefinita.

Nota:

- Le porte di rete virtuali non sono supportate. Non utilizzare una porta di rete fisica per simulare più porte di rete virtuali.
- Quando l'impostazione di rete del server è configurata su AUTO, XClarity Administrator può rilevare automaticamente le porte di rete negli slot 1-16. Almeno una porta negli slot 1-16 deve disporre di una connessione a XClarity Administrator.
- Se si desidera utilizzare una porta di rete nello slot 17 o superiore per l'indirizzo MAC, non è possibile utilizzare l'opzione AUTO. È necessario invece configurare l'impostazione di rete del server con l'indirizzo MAC della porta specifica che si desidera utilizzare.
- Per i server ThinkServer, non tutti gli indirizzi MAC host sono visualizzati. In molti casi, gli indirizzi MAC per gli adattatori Ethernet AnyFabric sono elencati nella finestra di dialogo Modifica impostazioni di rete. Gli indirizzi MAC per gli altri adattatori Ethernet (ad es. Lan-On-Motherboard) non sono elencati. Nei casi in cui l'indirizzo MAC per un adattatore non è disponibile, utilizzare il metodo AUTO per le distribuzioni non VLAN.

- Indirizzo IP e maschera di sottorete
- Gateway IP
- Fino a due server DNS (Domain Name System)
- Velocità MTU (Maximum Transmission Unit)
- ID VLAN, se la modalità IP VLAN è abilitata

Se si decide di utilizzare VLAN, è possibile assegnare un ID VLAN alla scheda di rete host configurata.

Procedura

Per configurare le impostazioni di rete per uno o più server, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.

Passo 2. Selezionare uno o più server da configurare. È possibile selezionare un massimo di 28 server da configurare contemporaneamente.

Passo 3. Fare clic su **Elementi selezionati modificati → Impostazioni di rete** per visualizzare la pagina Modifica impostazioni di rete.

Passo 4. Completare i campi nella tabella per ciascun server.

Suggerimento: in alternativa alla compilazione delle singole righe, è possibile aggiornare tutte le righe nella tabella per alcuni dei campi:

a. Fare clic su **Modifica tutte le righe → Nome host** per inviare i nomi host a tutti i server utilizzando uno schema di denominazione predefinito o personalizzato.

b. Fare clic su **Modifica tutte le righe → Indirizzo IP** per assegnare un intervallo di indirizzi IP, maschere di sottorete e gateway. L'indirizzo IP assegnato a ciascun server, a iniziare dal primo indirizzo IP e fino all'ultimo indirizzo IP visualizzato. La maschera di sottorete e l'indirizzo IP del gateway vengono applicati a ciascun server.

c. Fare clic su **Modifica tutte le righe → DNS (Domain Name System)** per impostare i server DNS che dovranno essere utilizzati dal sistema operativo per la ricerca DNS. Se la rete definisce i server DNS automaticamente, oppure se non si desidera definire i server DNS, selezionare **Nessuno**.

d. Fare clic su **Modifica tutte le righe → MTU (Maximum Transmission Unit)** per impostare la MTU da utilizzare sull'adattatore Ethernet configurato nel sistema operativo distribuito.

e. Fare clic su **Modifica tutte le righe → ID VLAN** per impostare un ID VLAN specifico per l'etichettatura VLAN del sistema operativo.

   È possibile specificare un valore compreso tra 1 e 4095. Il valore predefinito è 1, ovvero la modalità VLAN non viene utilizzata.

   Questa opzione è disponibile solo se Usa VLAN è abilitato nella finestra di dialogo Impostazioni globali (vedere Configurazione delle impostazioni globali di distribuzione del sistema operativo).

   Importante:

   - Specificare un ID VLAN soltanto quando è necessaria un'etichetta VLAN per il funzionamento sulla rete. L'utilizzo di etichette **VLAN** può incidere sull'instradabilità tra il sistema operativo host e XClarity Administrator.
   - Gli switch chassis o ToR (Top-of-Rack) devono essere configurati in modo indipendente per gestire i pacchetti etichettati VLAN. Assicurarsi che XClarity Administrator e la rete di dati sia configurata in modo da gestire tali pacchetti correttamente.
   - La modalità VLAN è supportata solo per i server che dispongono di indirizzi MAC nell'inventario. Se AUTO è l'unico indirizzo MAC disponibile per un server, non è possibile utilizzare le VLAN per distribuire i sistemi operativi a tale server.
   - L'etichettatura VLAN non è supportata per le distribuzioni del sistema operativo Linux. Tuttavia, se si desidera eseguire la distribuzione con VLAN su alcuni server e contemporaneamente anche in altri server senza VLAN, è possibile forzare la distribuzione in modalità VLAN impostando l'ID VLAN su 1.

Passo 5. Fare clic su **OK** per salvare le impostazioni. Le impostazioni vengono salvate e sono permanenti solo nella cache di storage locale del browser Web.

Risultati

Ogni server configurato ora mostra **Pronto** come stato di distribuzione nella pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.

Scelta della posizione di storage per i server gestiti

Scegliere la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo per uno o più server.

Prima di iniziare

Esaminare le considerazioni sullo storage e sulle opzioni di avvio prima di scegliere la posizione di storage (vedere Considerazioni sulla distribuzione del sistema operativo).

È possibile distribuire un sistema operativo sui seguenti tipi di storage:

- **Unità disco locale**

  Sono supportati solo dischi collegati a un controller RAID o HBA SAS/SATA.

  Lenovo XClarity Administrator installa l'immagine del sistema operativo sul primo disco RAID locale enumerato nel server gestito.

  Se la configurazione RAID sul server non è configurata correttamente o se è inattiva, Lenovo XClarity Administrator potrebbe non vedere il disco locale. Per risolvere il problema, abilitare la configurazione

RAID tramite i pattern di configurazione (vedere Definizione di storage locale) o tramite il software di gestione RAID sul server.

Nota:

- Se è presente anche un'unità M.2, l'unità disco locale deve essere configurata per la modalità RAID hardware.
- Se è abilitato un adattatore SATA, la modalità SATA *non* deve essere impostata su "IDE".
- Per i server ThinkServer, i sistemi operativi possono essere distribuiti solo sul disco locale. Lo storage SAN e gli hypervisor incorporati non sono supportati.
- Per i server ThinkServer, la configurazione è disponibile solo mediante il software di gestione RAID sul server.

Per uno scenario di esempio per la distribuzione VMware ESXi 5.5 su un'unità disco installata in locale, vedere Distribuzione di ESXi su un'unità disco fisso locale.

- **(Solo ESXi) Hypervisor incorporato (adattatore supporti SD o USB)**

  Questa posizione è applicabile solo se è in corso la distribuzione di un'immagine VMware ESXi sui server gestiti.

  Uno dei seguenti dispositivi può fungere da hypervisor incorporato:

  - Chiave USB di licenza IBM (PN 41Y8298) o chiave USB di licenza Lenovo montata in una porta per utilizzo specifico su uno dei server seguenti:
    - Flex System x222
    - Flex System x240
    - Flex System x440
    - Flex System x480
    - Flex System x880
    - System x3850 X6
    - System x3950 X6
  - Adattatore supporti SD installato nei server seguenti:
    - Flex System x240 M5
    - System x3500 M5
    - System x3550 M5
    - System x3650 M5

    Inoltre, l'unità deve essere configurata come segue:
    - Le unità appropriate sull'adattatore supporti devono essere definite.
    - La modalità dell'adattatore supporti SD deve essere impostata su **Operativo**.
    - Il proprietario deve essere impostato su Sistema oppure Solo sistema.
    - L'accesso deve essere impostato su Lettura/Scrittura.
    - Un numero LUN di 0 deve essere assegnato all'unità.

    Importante: se l'adattatore supporti SD non è configurato correttamente, la distribuzione del sistema operativo sull'adattatore supporti SD da Lenovo XClarity Administrator non verrà completata correttamente.

    È possibile modificare la modalità dell'adattatore supporti SD su **Configurazione** e configurare l'adattatore supporti mediante il controller di gestione CLI utilizzando il comando `sdraid`. Per ulteriori informazioni sull'impostazione della modalità dell'adattatore supporti SD e sulla configurazione dell'adattatore dalla CLI, vedere la Documentazione online di Integrated Management Module II.

Se sul server gestito sono installate due chiavi hypervisor, il programma di installazione VMware seleziona la prima chiave enumerata per la distribuzione.

Nota: il tentativo di distribuzione di Microsoft Windows su un server gestito con una chiave hypervisor installata potrebbe causare problemi anche se non si seleziona la chiave dell'hypervisor incorporato. Se si verificano errori nella distribuzione Windows, rimuovere la chiave dell'hypervisor incorporato dal server gestito e tentare nuovamente la distribuzione di Microsoft Windows sul server.

- **Unità M.2**

  Lenovo XClarity Administrator installa l'immagine del sistema operativo nella prima unità M.2 configurata sul server gestito.

  Lo storage M.2 è supportato solo sui server ThinkSystem.

  Attenzione: Se un dispositivo gestito dispone di entrambe le unità locali (SATA, SAS o SSD) non configurate per la modalità RAID hardware e per le unità M.2, è necessario disabilitare le unità locali se si desidera utilizzare l'unità M.2 oppure è necessario disabilitare le unità M.2 se si desidera utilizzare le unità locali. È possibile disabilitare i dispositivi del controller di storage integrato e le ROM dell'opzione di storage UEFI e legacy mediante i pattern di configurazione, selezionando "Disabilita disco locale" nella scheda "Storage locale" della procedura guidata o creando un pattern di configurazione da un server esistente e quindi disabilitando i dispositivi M.2 nel pattern UEFI esteso.

- **Storage SAN**

  Lenovo XClarity Administrator installa l'immagine del sistema operativo sulla destinazione di avvio SAN configurata sul server gestito.

  Sono supportati i seguenti protocolli.
  - Fibre Channel
  - Fibre Channel over Ethernet
  - SAN iSCSI (solo utilizzando l'adattatore Emulex VFA5.2 2x10 GbE SFP+ e FCoE/iSCSI SW o l'adattatore Emulex VFA5.2 ML2 2x10 GbE SFP+ e gli adattatori FCoE/iSCSI SW)

  Sui server rack gestiti, è possibile distribuire solo Windows o RHEL nello storage SAN. Verificare che la destinazione di avvio SAN sia configurata sui server gestiti. È inoltre possibile configurare la destinazione di avvio SAN FC utilizzando un pattern server (vedere Definizione delle opzioni di avvio)

  Nella distribuzione VMware ESXi:

  - I dischi fissi locali devono essere disabilitati o rimossi dal server. È possibile disabilitare i dischi fissi locali utilizzando i pattern server (vedere Definizione di storage locale).
  - Se sono disponibili più volumi SAN, per la distribuzione viene utilizzato solo il primo volume.

  Verificare che il volume del sistema operativo su cui si sta eseguendo l'installazione sia l'unico volume visibile dal sistema operativo.

  Per uno scenario di esempio per la distribuzione VMware ESXi 5.5 sui volumi SAN collegati ai server, vedere Distribuzione di ESXi su storage SAN.

Nota: Ciascun server deve essere dotato di un adattatore RAID hardware o di HBA SAS/SATA installato e configurato. Il software RAID generalmente presente sull'adattatore di storage SATA Intel integrato o lo storage configurato come JBOD non è supportato. Tuttavia, se non è presente un adattatore RAID hardware, in alcuni casi potrebbe essere possibile abilitare la modalità **SATA AHCI** dell'adattatore SATA per la distribuzione del sistema operativo oppure impostare i dischi validi non configurati su JBOD. Per ulteriori informazioni, vedere Il programma di installazione del sistema operativo non riesce a trovare il disco su cui si desidera installare XClarity Administrator nella documentazione online di XClarity Administrator.

Procedura

Per scegliere la posizione di storage di uno o più server gestiti, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci immagini sistema operativo.

Passo 2. Selezionare i server per i quali si desidera modificare le impostazioni di storage.

Passo 3. Fare clic su **Modifica elementi selezionati → Posizione di storage** per modificare l'ordine di priorità delle posizioni di storage per tutti i server selezionati. Se la prima posizione di storage non è compatibile viene tentata la posizione di storage successiva.

È possibile impostare la priorità per le seguenti posizioni di storage:
- **Utilizza storage unità disco locali**
- **Utilizza hypervisor incorporato (adattatore supporti SD o USB) quando ESXi è selezionato**
- **Usa unità M.2**
- **Usa storage SAN**

Passo 4. Per ciascun server, selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**. È possibile scegliere tra i seguenti valori, che corrispondono ai valori del passaggio precedente.
- **Unità disco locale**
- **Hypervisor incorporato**
- **Unità M.2**
- **Storage SAN**

Se si seleziona **Storage SAN**, viene visualizzata una finestra di dialogo per configurare il volume SAN. Verificare che il volume SAN di destinazione sia raggiungibile durante la distribuzione.

Se la posizione di storage selezionata non è compatibile con il server, Lenovo XClarity Administrator tenta la distribuzione del sistema operativo sulla posizione di storage successiva secondo la priorità definita nel passaggio precedente.

Distribuzione di un'immagine del sistema operativo

È possibile utilizzare Lenovo XClarity Administrator per distribuire un'immagine del sistema operativo simultaneamente su un massimo di 28 server.

Prima di iniziare

Leggere le relative considerazioni sulla distribuzione del sistema operativo prima di tentare di distribuire i sistemi operativi sui server gestiti (vedere Considerazioni sulla distribuzione del sistema operativo).

Nella scheda **Immagini sistema operativo** verificare che lo **Stato distribuzione** del sistema operativo da distribuire sia impostato su "Pronto." Per distribuire il sistema operativo Windows, è necessario un file di avvio di WinPE. Se non è disponibile un file di WinPE corrispondente, lo **Stato distribuzione** è impostato su "Non pronto" e il sistema operativo non può essere distribuito. È necessario scaricare manualmente e importare un file di WinPE (vedere Importazione dei file di avvio).

Dalla scheda **Gestisci immagini sistema operativo** è possibile filtrare l'elenco di immagini del sistema operativo facendo clic su **Mostra tutto → Stato distribuzione**. È possibile filtrare l'elenco per mostrare solo i server con stato "Pronto," "Non pronto," e "Avvertenza". Nota: se lo stato di distribuzione di un'immagine del sistema operativo è "Non pronto", il sistema operativo non è incluso nell'elenco dei sistemi operativi distribuibili.

Per impostazione predefinita sono supportate le impostazioni locali relative alla lingua inglese. Per specificare le impostazioni locali specifiche di una lingua, è necessario utilizzare un file di configurazione personalizzato e un file di installazione automatica. Per ulteriori informazioni, vedere Distribuzione di SLES 12 SP3 con i server NTP e le impostazioni locali configurabili, Distribuzione di Windows 2016 in giapponese.

la distribuzione del sistema operativo su uno storage non RAID non è supportata.

Attenzione: Se il server dispone attualmente di un sistema operativo installato, la distribuzione dell'immagine del sistema operativa sovrascriverà il sistema operativo corrente.

Per i server con XCC2 con Protezione del sistema abilitato e l'azione impostata su **Impedisci avvio del sistema operativo**, verificare che Protezione del sistema sia conforme sul dispositivo. Se Protezione del sistema non è conforme, ai dispositivi viene impedito il completamento del processo di avvio, determinando un errore della distribuzione del sistema operativo. Per eseguire il provisioning di questi dispositivi, rispondere manualmente al prompt di avvio di Protezione del sistema per consentire l'avvio normale dei dispositivi.

Procedura

Per distribuire un'immagine del sistema operativo su uno o più server gestiti, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.

Suggerimento: per i complessi scalabili, il sistema operativo viene distribuito sulla partizione primaria; pertanto, solo la partizione primaria è inclusa nell'elenco server.

Passo 2. Selezionare uno o più server su cui deve essere distribuito il sistema operativo. È possibile distribuire un sistema operativo su un massimo di 28 server alla volta.

È possibile ordinare le colonne della tabella per semplificare l'identificazione di server specifici. Inoltre, è possibile filtrare l'elenco dei dispositivi visualizzati, selezionando un'opzione nel menu **Mostra** per elencare solo i dispositivi di uno chassis, un rack o un gruppo specifico oppure immettendo il testo (ad esempio, un nome o un indirizzo IP) nel campo **Filtro**.

Suggerimento: se si desidera distribuire lo stesso sistema operativo su tutti i nodi di elaborazione è possibile scegliere più nodi di elaborazione da chassis differenti.

Passo 3. Per configurare le impostazioni di rete, fare clic su **Modifica elementi selezionati → Impostazioni di rete**.

Per ulteriori informazioni, vedere Configurazione delle impostazioni di rete per i server gestiti.

Passo 4. Per ciascun server, selezionare il profilo dell'immagine del sistema operativo da distribuire nell'elenco a discesa **Immagine da distribuire**.

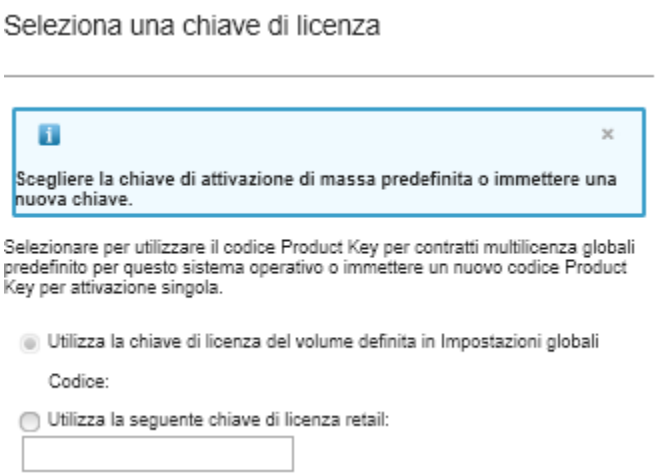
Accertarsi di selezionare un profilo di immagine del sistema operativo compatibile con il server selezionato. È possibile determinare la compatibilità dagli attributi del profilo elencati nella colonna **Attributo** della pagina Gestisci immagini sistema operativo. Per informazioni sugli attributi del profilo, vedere Profili immagine del sistema operativo.

Passo 5. Per ciascun server, fare clic sull'icona **Chiave di licenza** ( ) e specificare la chiave di licenza da utilizzare per attivare il sistema operativo dopo l'installazione.

XClarity Administrator supporta i codici Product Key per contratti multilicenza globali predefiniti per le installazioni Windows e i codici Product Key per attivazione singola per Windows e VMware ESXi.

Per utilizzare il codice Product Key per contratti multilicenza globale specificato nella finestra di dialogo Impostazioni globali, selezionare **Utilizza la chiave di licenza del volume definita in Impostazioni globali**. Per ulteriori informazioni sui codici Product Key per contratti multilicenza globali, vedere Configurazione delle impostazioni globali di distribuzione del sistema operativo.

Per utilizzare un codice Product Key per attivazione singola, selezionare **Utilizza la seguente chiave di licenza retail** e immettere la chiave nel seguente campo.



Passo 6. **Facoltativo:** se è stato selezionato un sistema operativo Windows per qualsiasi server, è possibile abbinare il sistema operativo Windows a un dominio di Active Directory come parte della distribuzione del sistema operativo facendo clic sull'icona **Cartella** ( ) visualizzata accanto all'immagine del sistema operativo e selezionando il nome di Active Directory.

Per utilizzare l'Active Directory predefinito specificato nella finestra di dialogo Impostazioni globali, selezionare **Utilizza Active Directory definito in Impostazioni globali**. Per ulteriori informazioni sull'abbinamento di un dominio di Active Directory, vedere Integrazione con Windows Active Directory.

Per utilizzare un Active Directory singolo, selezionare **Utilizza il seguente Active Directory** e selezionare il dominio di Active Directory.

Passo 7. Per ciascun server, selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.
- **Unità disco locale**
- **Hypervisor incorporato**
- **Unità M.2**
- **Storage SAN**

Se la posizione di storage selezionata non è compatibile con il server, XClarity Administrator tenta la distribuzione del sistema operativo sulla posizione di storage successiva in base alla priorità.

Nota: per i server ThinkServer, è disponibile solo l'opzione **Disco locale**

Per ulteriori informazioni su come configurare la posizione di storage, vedere Scelta della posizione di storage per i server gestiti.

Nota: per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.

Passo 8. Verificare che lo stato di distribuzione per tutti i server selezionati sia Pronto.

Importante: verificare che lo stato di distribuzione di tutti i server selezionati sia Pronto. Se lo stato di un server è Non pronto, non è possibile distribuire un'immagine del sistema operativo sul server selezionato. Fare clic sul collegamento **Non pronto** per ottenere informazioni utili alla risoluzione del problema. Se le impostazioni di rete non sono valide, fare clic su **Modifica elementi selezionati → Impostazioni di rete** per configurare le impostazioni di rete.

Passo 9. Fare clic sull'icona **Distribuisci immagini** ( ) per avviare la distribuzione del sistema operativo.

Se sono state aggiunte impostazioni di configurazione personalizzate al profilo immagine del sistema operativo, viene visualizzata la scheda **Impostazioni personalizzate** nella finestra di dialogo Distribuisci immagine sistema operativo. Specificare le impostazioni personalizzate, impostazioni comuni del server e le impostazioni specifiche del server, quindi fare clic su **Avanti** per continuare la distribuzione del sistema operativo. Tenere presente che la distribuzione del sistema operativo non proseguirà se non viene specificato l'input per le impostazioni di configurazione personalizzate richieste.

Al termine

È possibile monitorare lo stato del processo di distribuzione dal log dei processi. Dal menu XClarity Administrator, fare clic su **Monitoraggio → Processi**. Per ulteriori informazioni sul log processi, vedere Monitoraggio dei processi.

è inoltre possibile configurare una sessione di controllo remoto mediante BMC affinché il server visualizzi l'avanzamento dell'installazione. Per ulteriori informazioni sul controllo remoto, vedere Utilizzo del controllo remoto per gestire i server Converged, Flex System, NeXtScale e System x.

Le informazioni sulla distribuzione vengono salvate per il sistema operativo. È possibile visualizzare le informazioni sulla distribuzione facendo clic su **Provisioning → Gestisci accesso al sistema operativo** e passando il puntatore del mouse sul nome del server.

Integrazione con Windows Active Directory

Quando si distribuisce un'immagine Windows utilizzando Lenovo XClarity Administrator, è possibile eseguire l'aggiunta a un dominio di Active Directory nell'ambito della distribuzione del sistema operativo.

Prima di iniziare

Per eseguire l'aggiunta a un dominio di Active Directory nell'ambito della distribuzione dell'immagine del sistema operativo Windows, è necessario configurare il server di gestione e il server Windows su cui è in esecuzione il controller del dominio di Active Directory interessato. Per eseguire questa configurazione, è necessario l'accesso seguente:

- Un account dell'amministratore con privilegi per l'autenticazione e l'aggiunta al dominio dei server Active Directory. Questo account deve disporre di privilegi simili a quelli del gruppo di amministratori di dominio predefinito e sarà possibile utilizzare un account in questo gruppo per questa configurazione.
- Accesso a un DNS (Domain Name System) che risolve al server Active Directory su cui è in esecuzione il controller di dominio. Questo DNS deve essere specificato nell'opzione **Impostazioni di rete → DNS** per il server su cui è in esecuzione la distribuzione del sistema operativo.
- L'amministratore del server Active Directory deve creare il nome del computer richiesto sul server di dominio prima della distribuzione del sistema operativo. Il tentativo di aggiunta non crea il nome del computer. Se non viene specificato un nome, l'aggiunta non riesce.
- L'amministratore del server Active Directory deve specificare il nome host del server su cui è in esecuzione la distribuzione dell'immagine come nome computer nell'unità organizzativa di destinazione facendo clic sul campo **Impostazioni di rete → Nome host**.

  Il nome host specificato (nome del computer) deve essere univoco. Se viene specificato un nome che è già in uso da un'altra installazione Windows, l'aggiunta non avrà esito positivo.

È possibile unire il dominio di Active Directory utilizzando uno dei seguenti metodi:

- **Utilizzare un dominio di Active Directory**

È possibile scegliere di utilizzare un dominio di Active Directory specifico da un elenco di domini predefiniti. Completare le seguenti operazioni per definire un dominio di Active Directory in XClarity Administrator. Se si desidera utilizzare più domini, ripetere queste operazioni per ciascun nome di dominio.

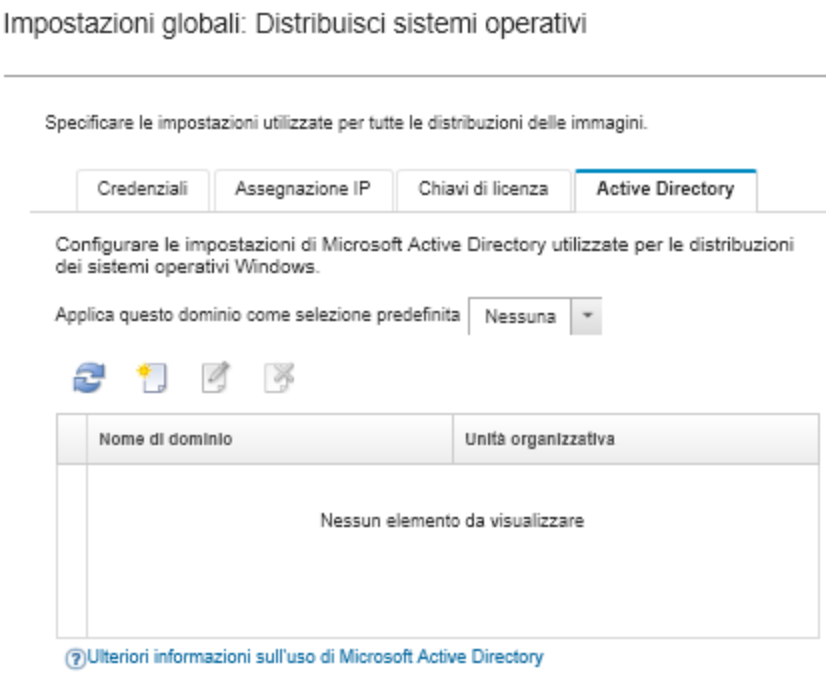
1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci immagini sistema operativo.
2. Fare clic sull'icona **Impostazioni globali** ( ) per visualizzare la finestra di dialogo Impostazioni globali: distribuisci sistemi operativi.
3. Fare clic sulla scheda **Active Directory**.
4. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo Aggiungi nuovo dominio di Active Directory.
5. Specificare il nome di dominio e l'unità organizzativa.

   La distribuzione del sistema operativo supporta l'aggiunta a un dominio e la creazione di unità organizzative annidate all'interno di un dominio. Se si specificano unità organizzative, non è necessario specificare esplicitamente l'unità organizzativa come parte dell'aggiunta. Active Directory può ricavare l'unità organizzativa corretta utilizzando il nome di dominio e il nome del computer.
6. Fare clic su **OK**.

- **Utilizzare il dominio di Active Directory predefinito**

  È possibile scegliere di utilizzare il dominio di Active Directory predefinito configurato nelle impostazioni globali. Completare le seguenti operazioni per impostare il dominio di Active Directory predefinito in XClarity Administrator.

  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci immagini sistema operativo.
  2. Fare clic sull'icona **Impostazioni globali** ( ) per visualizzare la finestra di dialogo Impostazioni globali: distribuisci sistemi operativi.
  3. Fare clic sulla scheda **Active Directory**.



4. Facoltativo: dal menu a discesa **Applica questo dominio come selezione predefinita**, selezionare il dominio di Active Directory da utilizzare per impostazione predefinita per ciascuna distribuzione Windows.
5. Fare clic su **OK**.

- **Utilizzare i dati BLOB dei metadati**

  È possibile utilizzare i metadati dell'account del computer Active Directory (in formato BLOB con codifica Base-64) per unire il dominio di Active Directory di qualsiasi server. Completare le seguenti operazioni per generare i dati BLOB dei metadati.

  1. Utilizzare un account di amministratore per eseguire il login al computer. Il computer deve essere parte del dominio di Active Directory a cui ci si sta aggiungendo.
  2. Fare clic su **Start → Programmi → Accessori**. Fare clic con il pulsante destro del mouse su **Prompt dei comandi**, quindi fare clic su **Esegui come amministratore**.
  3. Spostarsi nella directory C:\windows\system32.
  4. Eseguire il comando `djoin` utilizzando il seguente formato per eseguire un'aggiunta di dominio offline:
     ```
     djoin /provision /domain <AD_domain_name> /machine <hostname> /savefile blob
     ```

     dove:

     – *<AD_domain_name>* è il nome del dominio di Active Directory.

     – *<hostname>* è il nome host del server su cui è in esecuzione la distribuzione dell'immagine come nome computer nell'unità organizzativa di destinazione facendo clic sul campo **Impostazioni di rete → Nome host**.

     Questo comando crea un file denominato `BLOB` che contiene i dati BLOB dei metadati. Il contenuto di questo file viene utilizzato dal processo di distribuzione del sistema operativo per specificare i dettagli dell'unione Active Directory, pertanto si consiglia di tenere questi dati a portata di mano.

     I dati BLOB dei metadati sono informazioni sensibili.

Per informazioni dettagliate sulla distribuzione di un'immagine del sistema operativo, vedere Distribuzione di un'immagine del sistema operativo.

Procedura

Per eseguire l'aggiunta a un dominio di Active Directory, completare le seguenti operazioni.

Passo 1. Importare l'immagine del sistema operativo Windows nel repository di immagini del sistema operativo (vedere Importazione delle immagini del sistema operativo).

Passo 2. Selezionare uno o più server su cui deve essere distribuito il sistema operativo. È possibile distribuire un sistema operativo su un massimo di 28 server alla volta.

Suggerimento: se si desidera distribuire lo stesso sistema operativo su tutti i nodi di elaborazione è possibile scegliere più nodi di elaborazione da chassis differenti.

Passo 3. Per configurare le impostazioni di rete, fare clic su **Modifica elementi selezionati → Impostazioni di rete**.

a. Fare clic su **Modifica tutte le righe → DNS (Domain Name System)** e specificare almeno un DNS che risolva il dominio di Active Directory.

b. Per ciascun server, specificare un nome host corrispondente a un nome computer esistente nel dominio e nell'unità organizzativa a cui esegue l'aggiunta.

Per ulteriori informazioni sulla configurazione delle impostazioni di rete, vedere Configurazione delle impostazioni di rete per i server gestiti.

Passo 4. Per ciascun server, selezionare l'immagine del sistema operativo Windows da distribuire nella colonna **Immagine da distribuire**. Accanto al nome dell'immagine vengono visualizzate una cartella e le icone delle chiavi di licenza.

Passo 5. Per ciascun server, fare clic sull'icona **Chiave di licenza** ( ) e specificare la chiave di licenza da utilizzare per attivare il sistema operativo dopo l'installazione:

Passo 6. Per ciascun server, fare clic sull'icona **Cartella** ( ) e specificare il dominio di Active Directory. È possibile scegliere uno dei seguenti valori:

- **Utilizza Active Directory definito in Impostazioni globali** per utilizzare il dominio predefinito.
- **Utilizza il seguente Active Directory** per selezionare un dominio specifico.
- **Utilizza dati di blocco dei metadati** per specificare il contenuto del file BLOB.

  I dati BLOB dei metadati contengono informazioni sensibili e non vengono visualizzati nel campo. Queste informazioni sono disponibili solo finché l'operazione di distribuzione non viene completata. Non è persistente.

Passo 7. Per ciascun server, selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.
- **Unità disco locale**
- **Hypervisor incorporato**
- **Unità M.2**
- **Storage SAN**

Se la posizione di storage selezionata non è compatibile con il server, XClarity Administrator tenta la distribuzione del sistema operativo sulla posizione di storage successiva in base alla priorità.

Per ulteriori informazioni su come configurare la posizione di storage, vedere Scelta della posizione di storage per i server gestiti.

Nota: per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.

Passo 8. Verificare che lo stato di distribuzione per tutti i server selezionati sia Pronto.

Se lo stato di un server è Non pronto, non è possibile distribuire un'immagine del sistema operativo sul server selezionato. Fare clic sul collegamento **Non pronto** per ottenere informazioni utili alla risoluzione del problema. Se le impostazioni di rete non sono valide, fare clic su **Elementi selezionati modificati → Impostazioni di rete** per configurare le impostazioni di rete.

Passo 9. Fare clic sull'icona **Distribuisci immagini** () per avviare la distribuzione del sistema operativo.

La finestra di dialogo Distribuisci conferma richiede le credenziali da utilizzare per l'autenticazione al server di Active Directory ed eseguire l'aggiunta al dominio. Per motivi di sicurezza, tali credenziali non vengono memorizzate in XClarity Administrator. È necessario fornire le credenziali per ciascuna distribuzione Windows che si aggiunge al dominio.

È possibile monitorare lo stato del processo di distribuzione dal log dei processi. Dal menu XClarity Administrator, fare clic su **Monitoraggio → Processi**. Per ulteriori informazioni sul log processi, vedere Monitoraggio dei processi.

Risultati

Al termine della distribuzione del sistema operativo, aprire un browser Web all'indirizzo IP specificato nella pagina Modifica impostazioni di rete ed eseguire l'accesso per continuare il processo di configurazione.

Scenari di distribuzione del sistema operativo

Utilizzare questi scenari per semplificare la personalizzazione e la distribuzione dei sistemi operativi per i server gestiti.

Distribuzione di RHEL con driver di dispositivo personalizzati

In questo scenario vengono installati il sistema operativo Red Hat Enterprise Linux (RHEL) e i driver di dispositivo aggiuntivi non disponibili nel sistema operativo di base. Viene utilizzato un profilo personalizzato che include i driver di dispositivo aggiuntivi. Il profilo personalizzato può quindi essere selezionato nella pagina "Distribuisci immagini sistema operativo".

Prima di iniziare

Quando si distribuiscono i sistemi operativi tramite Lenovo XClarity Administrator, il sistema operativo deve includere i driver di dispositivo dell'adattatore di storage, Fibre Channel ed Ethernet corretti per l'hardware. Se un driver di dispositivo non è incluso nel sistema operativo, l'adattatore non è supportato per la distribuzione del sistema operativo. In XClarity Administrator v1.2.0 e versioni successive, è possibile personalizzare un sistema operativo aggiungendo i driver di dispositivo.

È possibile ottenere i driver di dispositivo da Pagina Web di Lenovo YUM Repository, dal fornitore (come Red Hat) oppure tramite un driver di dispositivo personalizzato, creato autonomamente. Per alcuni driver di dispositivo Windows, è possibile generare un driver di dispositivo personalizzato estraendo il driver di dispositivo dal file .exe di installazione nel sistema locale e creando un file di archivio .zip.

Nota: I driver di dispositivo RHEL devono essere in formato immagine .rpm o .iso.

Procedura

Per distribuire RHEL con i driver di dispositivo personalizzati, completare la seguente procedura.

Passo 1. Scaricare nel sistema locale il sistema operativo RHEL base dal sito Red Hat e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine RHEL da importare (ad esempio, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 2. Scaricare i driver di dispositivo personalizzati nel sistema locale e importare i file nel repository di immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione dei driver di dispositivo.

1. Fare clic sulla scheda **Driver di dispositivo**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `RHEL` per il sistema operativo.
5. Selezionare la versione del sistema operativo.
6. Selezionare il tipo di dispositivo.
7. Fare clic su **Sfoglia** per individuare e selezionare il driver di dispositivo da importare (ad esempio, `kmod-i40e-2.0.12-1.el7.x86_64.rpm`).
8. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

Passo 3. Creare un profilo immagine del sistema operativo personalizzato che include i driver di dispositivo personalizzati. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare un profilo immagine del sistema operativo da personalizzare (ad esempio, `Virtualization`).
3. Fare clic sull'icona **Crea** () per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio, `RHEL personalizzato con driver di dispositivo`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.
   c. Selezionare **Nessuno** per il tipo di personalizzazione.
   d. Fare clic su **Avanti**.
5. Nella scheda **Opzioni driver**, selezionare i driver di dispositivo personalizzati da includere nel profilo e fare clic su **Avanti** . Per impostazione predefinita sono inclusi i driver di dispositivo base.
6. Nella scheda **Software** fare clic su **Avanti**.

7. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato.

Passo 4. Distribuire il profilo immagine del sistema operativo personalizzato ai server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento: le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, *<base_OS>*|*<timestamp>*`_RHEL personalizzato con driver di dispositivo`) dall'elenco a discesa nella colonna **Immagine da distribuire**.

      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.
   d. (Facoltativo) Fare clic sull'icona **Chiave di licenza** () e specificare la chiave di licenza da utilizzare per attivare il sistema operativo dopo l'installazione.
   e. Selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.

      Nota: Per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.
   f. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.
3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** () per avviare la distribuzione del sistema operativo.
4. Nella scheda **Riepilogo**, verificare le impostazioni.
5. Fare clic su **Distribuisci** per distribuire il sistema operativo.

Distribuzione di RHEL e di un'applicazione Hello World PHP mediante un file di installazione automatica personalizzato

In questo scenario vengono installati il sistema operativo RHEL e il software personalizzato (Apache HTTP, PHP e un'applicazione Hello World PHP). Viene utilizzato un profilo immagine del sistema operativo personalizzato che include il file di installazione automatica personalizzato e uno script post-installazione che registrano il sistema operativo con il servizio di sottoscrizione Lenovo RHEL interno, in modo che sia possibile utilizzare i repository YUM, installare i pacchetti Apache e PHP, configurare il firewall per consentire le connessioni Apache, creare un'applicazione Hello World PHP e copiare la directory del server Web Apache e configurare i file di configurazione Apache per supportare PHP.

Prima di iniziare

È possibile distribuire RHEL con il software personalizzato in vari modi. In questo esempio viene utilizzato un file di installazione automatica personalizzato da includere nel profilo immagine del sistema operativo personalizzato. È inoltre possibile utilizzare uno script post-installazione che installa il software personalizzato importato nel repository e include il profilo immagine del sistema operativo personalizzato. Per installare il software mediante uno script post-installazione, vedere Distribuzione di RHEL e di un'applicazione Hello World PHP mediante software personalizzato e uno script post-installazione.

In questo scenario viene utilizzato il seguente file di esempio.

- RHEL_installSoftware_customUnattend.cfg Questo file di installazione automatica personalizzato utilizza i valori nelle macro predefinite e personalizzate e installa e configura il software personalizzato.

Procedura

Per distribuire RHEL con il software personalizzato mediante un file di installazione automatica personalizzato, completare le seguenti operazioni.

Passo 1. Scaricare nel sistema locale il sistema operativo RHEL base dal sito Red Hat e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine RHEL da importare (ad esempio, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 2. Modificare il file di installazione automatica RHEL (Kickstart) per registrare il sistema operativo con il servizio di sottoscrizione RHEL Satellite, installare i pacchetti HTTP (Apache) e PHP, creare una semplice applicazione Hello World PHP, aggiungere le macro predefinite richieste e altre macro predefinite, dove applicabile, come indirizzo IP, gateway, DNS e impostazioni del nome host e quindi importare il file personalizzato nel repository di immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione di file di installazione automatica personalizzati.

Aggiungere i comandi per registrare l'host con RHEL Satellite, ad esempio:

```
rpm -Uvh http://<YOUR_SATELLITE_SERVER_IP>/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="<YOUR_ORGANIZATION>" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms
```

Importante: Nel file di installazione automatica di esempio, specificare l'indirizzo IP del server satellite e dell'organizzazione in base alla configurazione del servizio di sottoscrizione.

Aggiungere i comandi per aggiornare l'host e per installare e configurare i pacchetti Apache e PHP, ad esempio:

```
%packages
@base
@core
@fonts
@gnome-desktop
@internet-browser
@multimedia
@x11
@print-client
-gnome-initial-setup

#Add the Apache and PHP packages
httpd
mod_ssl
openssl
```

```
php
php-mysql
php-gd
%end

yum -y update

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload

echo "<?PHP
echo 'Hello World !! ';
?>" | tee /var/www/html/index.php

sudo cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original

sudo sed -i -e 's/^[ \t]*//' /etc/httpd/conf/httpd.conf
sudo sed -i "s|IncludeOptional|#IncludeOptional|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|#ServerName www.example.com:80|ServerName localhost|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|DirectoryIndex index.html|DirectoryIndex index.html index.php|" /etc/httpd/conf/httpd.conf

echo "AddType application/x-httpd-php .php" | tee -a /etc/httpd/conf/httpd.conf
```

Nota: Il file di installazione automatica di esempio modifica i pacchetti predefiniti installati con il file Kickstart. Specifica i pacchetti Apache e PHO nell'ambito della sezione %packages.

Solo per ESXi e RHEL, XClarity Administrator fornisce la macro **#predefined.unattendSettings.networkConfig#** che aggiunge tutte le impostazioni di rete definite nell'interfaccia utente al file di installazione automatica e la macro **#predefined.unattendSettings.storageConfig#** che aggiunge tutte le impostazioni di storage definite nell'interfaccia utente al file di installazione automatica. Il file di installazione automatica di esempio contiene già queste macro.

XClarity Administrator fornisce anche alcune utili macro di base, come aggiunta di driver OOB, report di stato, script post-installazione e software personalizzato. Tuttavia, per sfruttare queste macro predefinite, è necessario specificare le seguenti macro nel file di installazione automatica personalizzato. Il file di esempio contiene già le macro richieste.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

Il file di esempio contiene già le macro richieste e le macro predefinite aggiuntive per specificare dinamicamente le impostazioni di rete per il server di destinazione e il fuso orario. Per ulteriori informazioni sull'aggiunta di macro ai file di installazione automatica, vedere Inserimento di macro predefinite e personalizzate in un file di installazione automatica.

È anche possibile aggiungere i comandi per inviare messaggi personalizzati al log dei processi in XClarity Administrator. Per ulteriori informazioni, vedere Aggiunta di report di stato personalizzato agli script di installazione.

Per importare lo script di installazione personalizzato, completare la seguente procedura. Per ulteriori informazioni, vedere Importazione di script di installazione personalizzati.

Per importare il file di installazione automatica personalizzato, completare la seguente procedura.

1. Fare clic sulla scheda **File di installazione automatica**.
2. Fare clic sull'icona **Importa** ( ).

3. Fare clic su **Importazione locale**.
4. Selezionare `RHEL` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file da importare (ad esempio, `RHEL_installSoftware_customUnattend.cfg`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

Passo 3. Creare un profilo immagine del sistema operativo personalizzato che include il software personalizzato e lo script post-installazione. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare un profilo immagine del sistema operativo da personalizzare (ad esempio, `Basic`).
3. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio, `Custom RHEL with software using custom unattend`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.
   c. Selezionare **Solo file di installazione automatica** per il tipo di personalizzazione.
   d. Fare clic su **Avanti**.
5. Nella scheda **Opzioni driver** fare clic su **Avanti**. Per impostazione predefinita sono inclusi i driver di dispositivo base.
6. Nella scheda **Software** fare clic su **Avanti**.
7. Nella scheda **File di installazione automatica**, selezionare il file di installazione automatica personalizzato (ad esempio, `RHEL_installSoftware_customUnattend.cfg`) e fare clic su **Avanti**.
8. Nella scheda **Script di installazione**, fare clic su **Avanti**.
9. Nella scheda **Riepilogo**, verificare le impostazioni.
10. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato.

Passo 4. Distribuire il profilo immagine del sistema operativo personalizzato ai server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento:

      - Le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
      - Le impostazioni di rete specificate nella finestra di dialogo "Impostazioni di rete" vengono aggiunte in fase di esecuzione al file di installazione automatica, utilizzando le macro **#predefined.hostPlatforms.networkSettings.<*setting*>#**.

   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, <*base_OS*>|<*timestamp*>`_RHEL personalizzato con software mediante un file di installazione automatica personalizzato`) dall'elenco a discesa nella colonna **Immagine da distribuire**.

      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.

d. (Facoltativo) Fare clic sull'icona **Chiave di licenza** ( ) e specificare la chiave di licenza da utilizzare per attivare il sistema operativo dopo l'installazione.

e. Selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.

   Nota: Per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.

f. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.

3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** ( ) per avviare la distribuzione del sistema operativo.
4. Nella scheda Impostazioni personalizzate, fare clic sulla scheda secondaria **Impostazioni di configurazione e di installazione automatica** e selezionare il file di installazione automatica personalizzato (ad esempio, `RHEL_installSoftware_customUnattend.cfg`).

5. Nella scheda **Riepilogo**, verificare le impostazioni.
6. Fare clic su **Distribuisci** per distribuire il sistema operativo.

Distribuzione di RHEL e di un'applicazione Hello World PHP mediante software personalizzato e uno script post-installazione

In questo scenario vengono installati il sistema operativo RHEL e il software personalizzato (Apache HTTP, PHP e un'applicazione Hello World PHP). Viene utilizzato un profilo immagine del sistema operativo personalizzato che include il software personalizzato e uno script post-installazione che registrano il sistema operativo con il servizio di sottoscrizione Lenovo RHEL interno, in modo che sia possibile utilizzare i repository YUM, installare i pacchetti Apache e PHP, configurare il firewall per consentire le connessioni Apache, creare un'applicazione Hello World PHP e copiare la directory del server Web Apache e configurare i file di configurazione Apache per supportare PHP. I pacchetti software personalizzati vengono esportati sull'host durante la distribuzione e possono essere utilizzati per lo script post-installazione personalizzato.

Prima di iniziare

È possibile distribuire RHEL e un'applicazione Hello World PHP in vari modi. In questo esempio viene utilizzato uno script post-installazione che installa il software personalizzato importato nel repository e include il profilo immagine del sistema operativo personalizzato. È inoltre possibile utilizzare un file di installazione automatica personalizzato da includere nel profilo immagine del sistema operativo personalizzato. Per installare il software mediante un file di installazione automatica personalizzato, vedere Distribuzione di RHEL e di un'applicazione Hello World PHP mediante un file di installazione automatica personalizzato.

In questo scenario vengono utilizzati i seguenti file di esempio.

- httpd.conf. Questo è il file di installazione di Apache HTTP.
- hello_world.php Questa è l'applicazione Hello World PHP.
- RHEL_installSoftware_customScript.sh Questo script post-installazione installa e configura il software personalizzato.

Nota:

- Gli script di installazione RHEL sono disponibili in uno dei seguenti formati: Bash (.sh), Perl (.pm o .pl), Python (.py)
- I file dei software e gli script di installazione vengono installati dal percorso dei file e dei dati personalizzati specificato durante la distribuzione. Il percorso predefinito di file e dati personalizzati è `/home/lxca`.

Procedura

Per distribuire RHEL con il software personalizzato mediante uno script post-installazione, completare le seguenti operazioni.

Passo 1. Scaricare nel sistema locale il sistema operativo RHEL base dal sito Red Hat e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine RHEL da importare (ad esempio, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 2. Scaricare il software personalizzato nel sistema locale e importare i file nel repository di immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione di software personalizzato.

Suggerimento: per importare il software personalizzato in XClarity Administrator, i file devono essere contenuti in un file tar.gz. Per questo esempio, comprimere i file di esempio `httpd.conf` e `index.php` in un file tar.gz denominato `RHEL_installSoftware_customsw.tar.gz` prima di continuare

1. Fare clic sulla scheda **Software**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `RHEL` per il sistema operativo.

5. Fare clic su **Sfoglia** per individuare e selezionare il file da importare (ad esempio, `RHEL_installSoftware_customsw.tar.gz`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

Passo 3. Creare uno script di post-installazione personalizzato e importare il file nel repository di immagini del sistema operativo.

Aggiungere i comandi per registrare l'host con RHEL Satellite, ad esempio:

```
rpm -Uvh http://satellite.labs.lenovo.com/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="Default_Organization" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms A
```

Aggiungere un comando per aggiornare l'host e installare e configurare i pacchetti Apache e PHP, ad esempio:

```
yum -y update
yum -y install httpd mod_ssl openssl php php-mysql php-gd

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

Aggiungere i comandi per aggiungere la nostra applicazione PHP al server Web Satellite, ad esempio:

```
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/lxca/index.php /var/www/html/index.php
```

Aggiungere i comandi per configurare Apache HTTP, ad esempio:

```
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/httpd.conf /etc/httpd/conf/httpd.conf
```

Tenere presente che questi comandi utilizzano macro predefinite per il percorso dei dati estratti e i file del software (**predefined.otherSettings.deployDataAndSoftwareLocation**).

È anche possibile aggiungere i comandi per inviare messaggi personalizzati al log dei processi in XClarity Administrator. Per ulteriori informazioni, vedere Aggiunta di report di stato personalizzato agli script di installazione.

Per importare lo script di installazione personalizzato, completare la seguente procedura. Per ulteriori informazioni, vedere Importazione di script di installazione personalizzati.

1. Fare clic sulla scheda **Script di installazione**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `RHEL` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare lo script post-installazione da importare (ad esempio, `RHEL_installSoftware_customScript.sh`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

Passo 4. Creare un profilo immagine del sistema operativo personalizzato che include il software personalizzato e lo script post-installazione. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare un profilo immagine del sistema operativo da personalizzare (ad esempio, `Basic`).

3. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio, `Custom RHEL with software using post-installation script`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.
   c. Selezionare **Nessuno** per il tipo di personalizzazione.
   d. Fare clic su **Avanti**.
5. Nella scheda **Opzioni driver** fare clic su **Avanti**. Per impostazione predefinita sono inclusi i driver di dispositivo base.
6. Nella scheda **Software**, selezionare i file di installazione del software (ad esempio, `httpd.conf` e `index.php`) e fare clic su **Avanti**.
7. Nella scheda **Script di installazione**, selezionare gli script di installazione (ad esempio, `RHEL_installSoftware_customScript.sh`) e fare clic su **Avanti**.
8. Nella scheda **Riepilogo**, verificare le impostazioni.
9. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato.

Passo 5. Distribuire il profilo immagine del sistema operativo personalizzato ai server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento: le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, *<base_OS>*|*<timestamp>*`_Custom RHEL with software using post-installation script`) dall'elenco a discesa nella colonna **Immagine da distribuire**

      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.
   d. Selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.

      Nota: Per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.
   e. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.
3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** ( ) per avviare la distribuzione del sistema operativo.
4. Nella scheda **Riepilogo**, verificare le impostazioni.
5. Fare clic su **Distribuisci** per distribuire il sistema operativo.

Distribuzione di SLES 12 SP3 con pacchetti personalizzati e fuso orario

In questo scenario vengono installati il sistema operativo SLES 12 SP3 (in inglese) e diversi pacchetti SLES facoltativi. Viene inoltre richiesto il fuso orario. Viene utilizzato un profilo immagine del sistema operativo

personalizzato che include un file di configurazione personalizzato e il file di installazione automatica. Questo profilo personalizzato può essere selezionato nella pagina "Distribuisci immagini sistema operativo". Quindi, è possibile selezionare i pacchetti SLE che si desidera distribuire e specificare il fuso orario nella scheda **Impostazioni personalizzate**. I valori selezionati vengono sostituiti alle macro personalizzate nel file di installazione automatica personalizzato e il programma di installazione di SLES AutoYaST utilizza questi valori per configurare il sistema operativo.

Prima di iniziare

In questo scenario vengono utilizzati i seguenti file di esempio.

- SLES_installPackages_customConfig.json. Questo file di configurazione richiede il fuso orario e i pacchetti SLES facoltativi (Linux, Apache, MySQL, pacchetto software PHP, pacchetto del server di posta SLES e pacchetto del file server SLES) da installare.
- SLES_installPackages_customUnattend.xml Questo file di installazione automatica utilizza i valori nelle macro predefinite e personalizzate definiti nel file di configurazione.

Procedura

Per distribuire SLES 12 SP3 sui server utilizzando un profilo immagine del sistema operativo personalizzato, completare le seguenti operazioni.

Passo 1. Scaricare nel sistema locale il sistema operativo SLES base dal sito Web SUSE e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ( ).
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine SLES 12 SP3 da importare (ad esempio, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 2. Creare un file delle impostazioni di configurazione personalizzate e importarlo nel repository di immagini del sistema operativo.

Il file delle impostazioni di configurazione è un file JSON che descrive i dati che devono essere raccolti dinamicamente durante il processo di distribuzione del sistema operativo. Per questo scenario, è necessario specificare i pacchetti SLES facoltativi che è possibile installare (come SLES Linux, Apache, MySQL, il pacchetto software PHP, il pacchetto del server di posta SLES e il pacchetto del file server SLES) e un fuso orario da utilizzare per ciascuna distribuzione del sistema operativo. Per ulteriori informazioni sulla creazione di un file delle impostazioni di configurazione, vedere Macro personalizzate.

Per importare il file delle impostazioni di configurazione, completare queste operazioni. Per ulteriori informazioni, vedere Importazione delle impostazioni di configurazione personalizzate.

1. Fare clic sulla scheda **File di configurazione**.
2. Fare clic sull'icona **Importa** ( ).
3. Fare clic su **Importazione locale**.

4. Selezionare `SLES` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file delle impostazioni di configurazione da importare (ad esempio, `SLES_installPackages_customConfig.json`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

   Nota: Quando si importa un file delle impostazioni di configurazione personalizzate, XClarity Administrator genera macro personalizzate per ogni impostazione nel file. È possibile aggiungere queste macro nel file di installazione automatica. Durante la distribuzione del sistema operativo, le macro vengono sostituite con i valori effettivi.

Passo 3. Modificare il file di installazione automatica di SLES per specificare i valori dinamici per i pacchetti SLES facoltativi e il fuso orario. Quindi importare il file personalizzato nel repository di immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione di file di installazione automatica personalizzati.

Nella sezione **<general>**, aggiungere le informazioni sul fuso orario, ad esempio:

```
<timezone>
   <hwclock></hwclock>
   <timezone></timezone>
</timezone>
```

Nella sezione **<patterns>**, aggiungere tre tag di pattern. Questi tag vengono utilizzati per le macro personalizzate delle impostazioni del pacchetto SLES facoltativo. Ad esempio:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern></pattern>
   <pattern></pattern>
   <pattern></pattern>
</patterns>
```

Nota:

- Questi tag sono nel file di installazione automatica di esempio.
- Quando si utilizza un file di installazione automatica personalizzato, XClarity Administrator non fornisce diverse funzioni utili, disponibili quando si usa un file di installazione automatica predefinito. Ad esempio, le destinazioni **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>** e **<UserAccounts>** for Administrator, **<Interfaces>** per la rete e l'elenco **<package>** per le funzioni di installazione devono essere specificati nel file di installazione automatica personalizzato in fase di caricamento.

Per importare il file di installazione automatica personalizzato, completare la seguente procedura.

1. Fare clic sulla scheda **File di installazione automatica**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.

4. Selezionare `SLES` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file di installazione automatica da importare (ad esempio, `SLES_installPackages_customUnattend.xml`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

   Nota: Viene visualizzata un'avvertenza per indicare che nel file di installazione automatica mancano le macro predefinite. Per ora, è possibile ignorare l'avvertenza. Le macro predefinite verranno aggiunte nel passaggio successivo
7. Fare clic su **Chiudi** nella finestra di dialogo dell'avvertenza per aprire la finestra di dialogo Modifica file di installazione automatica.

Passo 4. Associare il file di installazione automatica personalizzato con il file delle impostazioni di configurazione personalizzate e aggiungere le macro predefinite e personalizzate richieste (impostazioni) dal file delle impostazioni di configurazione al file di installazione automatica. Per ulteriori informazioni, vedere Associazione di un file di installazione automatica con un file delle impostazioni di configurazione, Inserimento di macro predefinite e personalizzate in un file di installazione automatica.

Suggerimento: è possibile associare facoltativamente il file di installazione automatica personalizzato con il file delle impostazioni di configurazione personalizzato e aggiungere le macro quando si importano i file di installazione automatica.

1. Dalla finestra di dialogo Modifica file di installazione automatica, selezionare il file delle impostazioni di configurazione per associare il file di installazione automatica dall'elenco a discesa **Associa un file di configurazione** (ad esempio, `SLES_installPackages_customConfig`).
2. Aggiungere le macro predefinite richieste al file di installazione automatica.
   a. Selezionare **Predefinito** dall'elenco a discesa **Macro disponibili**.
   b. Posizionare il cursore in un punto qualsiasi del file di installazione automatica dopo la riga 1 (dopo il tag **<xml>**).
   c. Espandere l'elenco **predefinito → unattendSettings** nell'elenco di macro predefinite.
   d. Fare clic sulle marco **preinstallConfig** e **postinstallConfig** per aggiungere le macro al file di installazione automatica.

   Ad esempio:

   ```
   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#
   <profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
   ```
3. Aggiungere la macro personalizzata per specificare il fuso orario.
   a. Selezionare **Personalizzato** dall'elenco a discesa **Macro disponibili**.
   b. Posizionare il cursore dopo il tag **<hwclock>** e fare clic su **timezone** per aggiungere la macro del fuso orario.
   c. Posizionare il cursore dopo il tag **<timezone>** e fare clic su **timezone** per aggiungere la macro del fuso orario.

   Ad esempio:

   ```
   <timezone>
      <hwclock>#timezone#</hwclock>
      <timezone>#timezone#</timezone>
   </timezone>
   ```
4. Aggiungere la macro personalizzata per specificare i pacchetti SLES facoltativi.
   a. Espandere l'elenco **impostazioni-server → nodo** nell'elenco di macro personalizzate.

b. Posizionare il cursore in uno dei tag **<pattern>** vuoti e fare clic su **fileserver**.

c. Posizionare il cursore in uno dei tag **<pattern>** vuoti e fare clic su **lampserver**.

d. Posizionare il cursore in uno dei tag **<pattern>** vuoti e fare clic su **mailserver**.

Ad esempio:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern>#server-settings.node.fileserver#</pattern>
   <pattern>#server-settings.node.lampserver#</pattern>
   <pattern>#server-settings.node.mailserver#</pattern>
</patterns>
```

5. Fare clic su **Salva** per associare i file e salvare le modifiche nel file di installazione automatica.

Passo 5. Creare un profilo immagine del sistema operativo personalizzato che include le impostazioni di configurazione personalizzate e i file di installazione automatica. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare un profilo immagine del sistema operativo da personalizzare (ad esempio, `Basic`).
3. Fare clic sull'icona **Crea** () per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio, `SLES personalizzato con pacchetti facoltativi`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.
   c. Selezionare **File delle impostazioni di configurazione e di installazione automatica associati** per il tipo di personalizzazione.
   d. Fare clic su **Avanti**.
5. Nella scheda **Opzioni driver** fare clic su **Avanti**. Per impostazione predefinita sono inclusi i driver di dispositivo base.
6. Nella scheda **Software** fare clic su **Avanti**.
7. Nella scheda **File di installazione automatica**, selezionare il file di installazione automatica (ad esempio, `SLES_installPackages_customUnattend.xml`) e fare clic su **Avanti**.

   Il file delle impostazioni di configurazione associato viene selezionato automaticamente.
8. Nella scheda **Script di installazione**, fare clic su **Avanti**.
9. Nella scheda **Riepilogo**, verificare le impostazioni.
10. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato.

Passo 6. Distribuire il profilo immagine del sistema operativo personalizzato ai server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

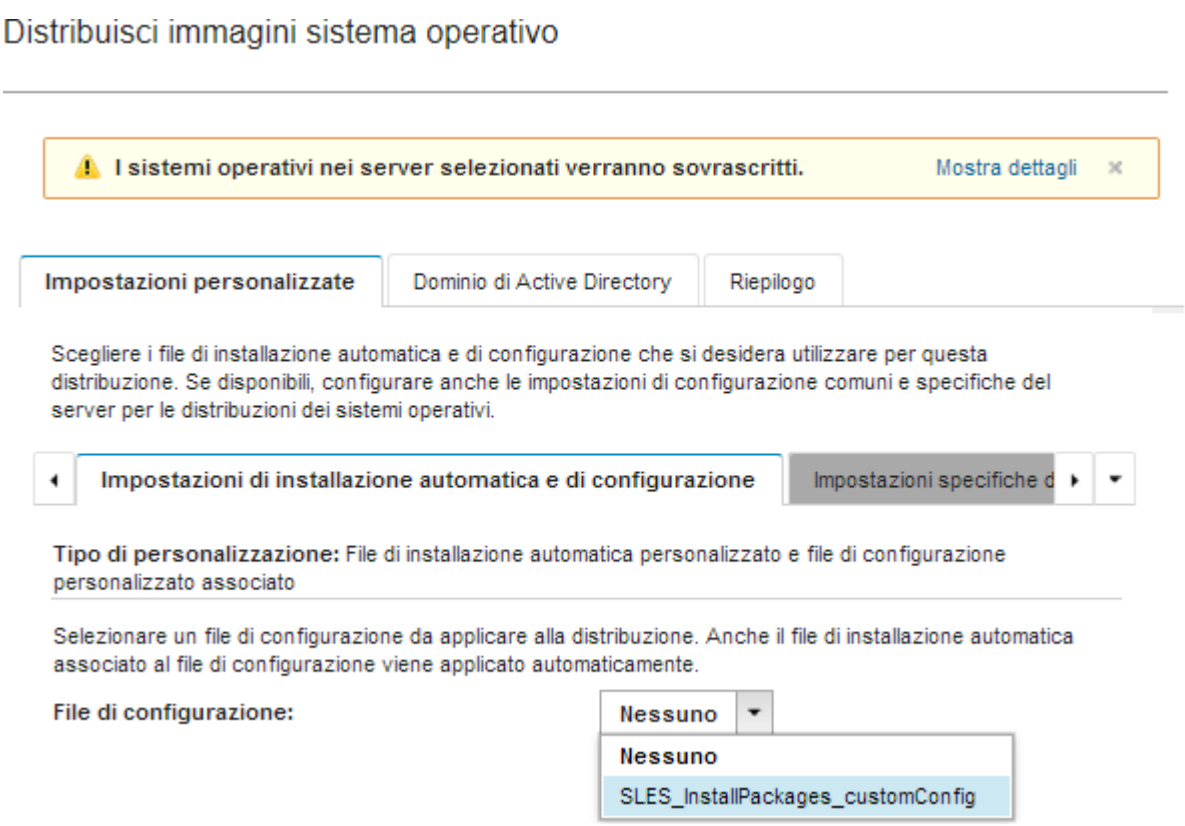
1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento: le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, <*base_OS*>|<*timestamp*>_SLES personalizzato con pacchetti facoltativi) dall'elenco a discesa nella colonna **Immagine da distribuire**

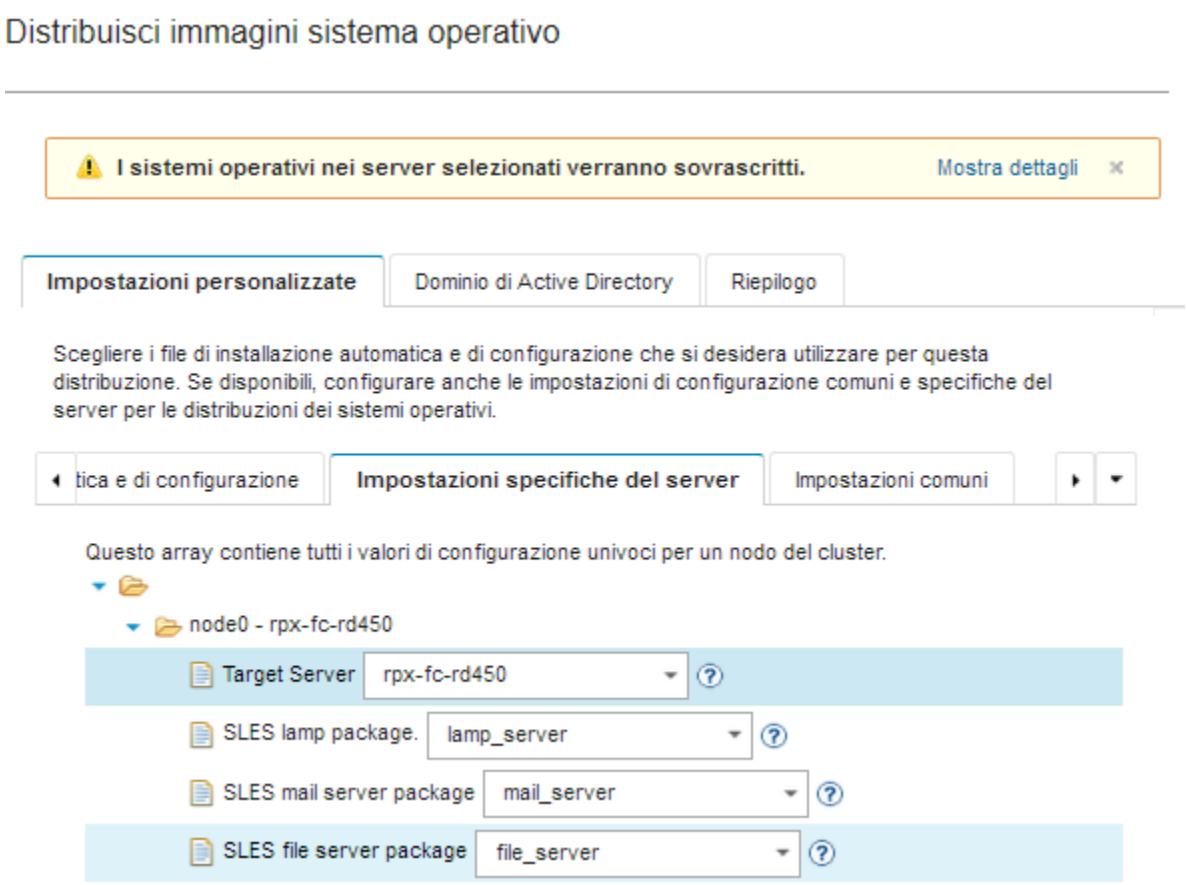
      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.
   d. Selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.

      Nota: Per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.
   e. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.
3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** () per avviare la distribuzione del sistema operativo.
4. Nella scheda **Impostazioni personalizzate**, fare clic sulla scheda secondaria **Impostazioni di configurazione e di installazione automatica** e selezionare il file delle impostazioni di configurazione personalizzato (ad esempio, SLES_installPackages_customConfig).

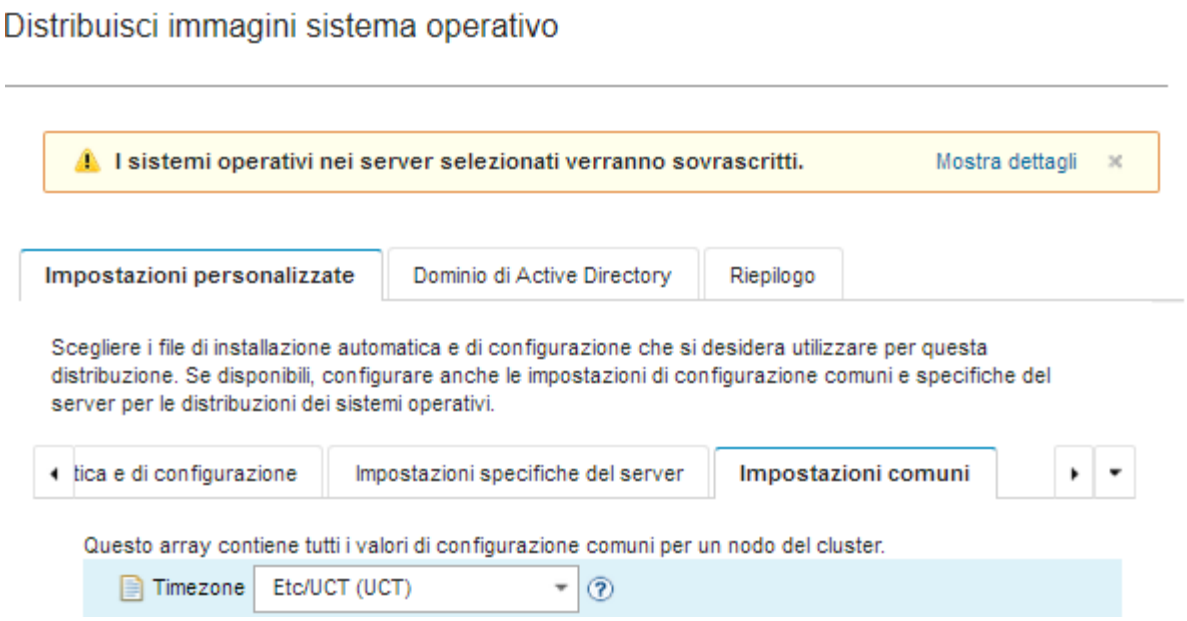
   Nota: Il file di installazione automatica personalizzato associato viene selezionato automaticamente.



5. Nella scheda secondaria **Impostazioni specifiche del server**, selezionare il server di destinazione e i pacchetti SLES facoltativi che si desidera distribuire.



6. Nella scheda secondaria **Impostazioni comuni**, selezionare il fuso orario da impostare per tutti i server di destinazione.



7. Nella scheda **Riepilogo**, verificare le impostazioni.
8. Fare clic su **Distribuisci** per distribuire il sistema operativo.

Distribuzione di SLES 12 SP3 con software personalizzato

In questo scenario vengono installati il sistema operativo SLES 12 SP3 e il software personalizzato (Java ed Eclipse IDE). Viene utilizzato un profilo personalizzato che include il software personalizzato e gli script post-installazione per installare e configurare il software personalizzato. I pacchetti software personalizzati vengono copiati sull'host durante la distribuzione e possono essere utilizzati per lo script post-installazione personalizzato.

Prima di iniziare

In questo scenario vengono utilizzati i seguenti file di esempio.

- jre-8u151-linux-x64.tar.gz. Questo è il file di installazione di Java per Eclipse.
- eclipse-4.6.3-3.1.x86_64.tar.gz Questo è il file di installazione di Eclipse IDE.
- SLES_installSoftware_customScript.sh Questo script post-installazione crea un utente per avviare Eclipse e installa Eclipse IDE e Java.

Nota:

- Gli script di installazione SLES sono disponibili in uno dei seguenti formati: Bash (.sh), Perl (.pm o .pl), Python (.py)
- I file dei software e gli script di installazione vengono installati dal percorso dei file e dei dati personalizzati specificato durante la distribuzione. Il percorso predefinito di file e dati personalizzati è `/home/lxca`.
- Per SLES 12 SP3, Eclipse IDE richiede il compilatore GCC, incluso nel profilo di base predefinito. Questo scenario crea un profilo personalizzato di immagine del sistema operativo personalizzato utilizzando il profilo di base predefinito come punto di partenza. Se si sceglie di utilizzare un altro profilo, è necessario verificare che il profilo includa il compilatore GCC.

Procedura

Per distribuire SLES 12 SP3 con software personalizzato, completare la seguente procedura.

Passo 1. Scaricare nel sistema locale il sistema operativo SLES 12 SP3 base dal sito Web SUSE e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ( ).
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine SLES 12 SP3 da importare (ad esempio, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 2. Scaricare il software personalizzato nel sistema locale e importare i file nel repository di immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione di software personalizzato.

1. Fare clic sulla scheda **Software**.
2. Fare clic sull'icona **Importa** ( ).
3. Fare clic su **Importazione locale**.
4. Selezionare `SLES` per il sistema operativo.

5. Fare clic su **Sfoglia** per individuare e selezionare il file da importare (ad esempio, `jre-8u151-linux-x64.tar.gz`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.
7. Fare clic nuovamente sull'icona **Importa** ().
8. Fare clic su **Importazione locale**.
9. Selezionare `SLES` per il sistema operativo.
10. Fare clic su **Sfoglia** per individuare e selezionare il file da importare (ad esempio, `eclipse-4.6.3-3.1.x86_64.tar.gz`).
11. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

Passo 3. Creare uno script di post-installazione personalizzato e importare il file nel repository di immagini del sistema operativo.

Aggiungere i comandi per creare un utente per avviare eclipse in questo file, ad esempio:

```
echo "Create a user called lenovo..."
egrep "lenovo" /etc/passwd >/dev/null
pass=$(perl -e 'print crypt($ARGV[0], "password")' "PasswOrd")
useradd -m -p $pass lenovo
[ $? -eq 0 ] &amp;amp;&amp;amp; echo "User has been created." || curl -X PUT
--globoff #predefined.otherSettings.statusSettings.urlStatus# -H "Content-Type: application/json"
-d '{"deployStatus":{"id":"46","parameters":["'"Could not create lenovo user"'"]}}'
--cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
--key #predefined.otherSettings.statusSettings.certLocation#/key.pem
--cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Aggiungere i comandi per installare il software, ad esempio:

```
#Install Java for eclipse
echo "Installing Java JRE 8...."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/jre-8u151-linux-x64.rpm

#Install eclipse
echo "Installing Eclipse IDE..."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/eclipse-4.6.3-3.1.x86_64.rpm
```

Tenere presente che questi comandi utilizzano macro predefinite per l'URL HTTPS che XClarity Administrator utilizza per segnalare lo stato (**predefined.otherSettings.statusSettings.urlStatus**), per la cartella contenente i certificati necessari per accedere al servizio web urlStatus dal sistema operativo host al primo avvio (**predefined.otherSettings.statusSettings.certLocation**) e per il percorso dei dati estratti e i file del software (**predefined.otherSettings. deployDataAndSoftwareLocation**).

È anche possibile aggiungere i comandi per inviare messaggi personalizzati al log dei processi inXClarity Administrator, come mostrato nel file di esempio. Per ulteriori informazioni, vedere Aggiunta di report di stato personalizzato agli script di installazione.

Per importare lo script di installazione personalizzato, completare la seguente procedura. Per ulteriori informazioni, vedere Importazione di script di installazione personalizzati.

1. Fare clic sulla scheda **Script di installazione**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `SLES` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare lo script post-installazione da importare (ad esempio, `SLES_installSoftware_customScript.sh`).

6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

Passo 4. Creare un profilo immagine del sistema operativo personalizzato che include il software personalizzato e lo script post-installazione. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare un profilo immagine del sistema operativo da personalizzare (ad esempio, `Basic`).
3. Fare clic sull'icona **Crea** () per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio, `SLES personalizzato con software`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.
   c. Selezionare **Nessuno** per il tipo di personalizzazione.
   d. Fare clic su **Avanti**.
5. Nella scheda **Opzioni driver** fare clic su **Avanti**. Per impostazione predefinita sono inclusi i driver di dispositivo base.
6. Nella scheda **Software**, selezionare i file di installazione del software (ad esempio, `jre-8u151-linux-x64.tar.gz` ed `eclipse-4.6.3-3.1.x86_64.tar.gz`) e fare clic su **Avanti**.
7. Nella scheda **Script di installazione**, selezionare gli script di installazione (ad esempio, `SLES_installSoftware_customScript.sh`) e fare clic su **Avanti**.
8. Nella scheda **Riepilogo**, verificare le impostazioni.
9. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato.

Passo 5. Distribuire il profilo immagine del sistema operativo personalizzato ai server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento: le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, <*base_OS*>|<*timestamp*>_`SLES personalizzato con software`) dall'elenco a discesa nella colonna **Immagine da distribuire**.

      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.
   d. Selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.

      Nota: Per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.
   e. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.
3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** () per avviare la distribuzione del sistema operativo.
4. Nella scheda **Riepilogo**, verificare le impostazioni.

5. Fare clic su **Distribuisci** per distribuire il sistema operativo.

Distribuzione di SLES 12 SP3 con i server NTP e le impostazioni locali configurabili

In questo scenario viene installato il sistema operativo SLES 12 SP3 in inglese, brasiliano o giapponese per la tastiera e le impostazioni locali del sistema operativo. Viene inoltre configurato l'indirizzo IP per un massimo di tre server NTP. Viene utilizzato un profilo immagine del sistema operativo personalizzato che include un file di installazione automatica (con macro predefinite e personalizzate) e un file delle impostazioni di configurazione per selezionare le impostazioni locali e del server NTP. Questo profilo personalizzato può essere selezionato nella pagina "Distribuisci immagini sistema operativo". Quindi, è possibile selezionare le impostazioni locali e del server NTP nella scheda **Impostazioni personalizzate**. I valori specificati vengono sostituiti alle macro personalizzate contenute nel file di installazione automatica personalizzato e il programma di installazione di SLES AutoYaST utilizza questi valori per configurare il sistema operativo.

Prima di iniziare

In questo scenario vengono utilizzati i seguenti file di esempio.

- SLES_locale_customConfig.json. Questo file di configurazione personalizzato richiede la lingua di installazione per la tastiera e le impostazioni locali del sistema operativo locale di SLES e del server NTP.
- SLES_locale_customUnattend.xml. Questo file di installazione automatica personalizzato utilizza i valori nelle macro personalizzate definiti nel file di configurazione.

Procedura

Per distribuire SLES 12 SP3 utilizzando un profilo immagine del sistema operativo personalizzato, completare le seguenti operazioni.

Passo 1. Scaricare nel sistema locale il sistema operativo SLES base dal sito Web SUSE e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ( ).
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine SLES 12 SP3 da importare (ad esempio, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata.

Passo 2. Creare un file delle impostazioni di configurazione personalizzate e importarlo nel repository di immagini del sistema operativo.

Il file delle impostazioni di configurazione è un file JSON che descrive i dati che devono essere raccolti dinamicamente durante il processo di distribuzione del sistema operativo. Per questo scenario, è necessario specificare le impostazioni locali del sistema operativo (en_US, ja_JP, pt_BR), le impostazioni locali della tastiera (inglese-us, giapponese o portoghese-br) e fino a tre indirizzi IP del server NTP da utilizzare per ogni distribuzione del sistema operativo. Per ulteriori informazioni sulla creazione di un file delle impostazioni di configurazione, vedere Macro personalizzate.

Per importare il file delle impostazioni di configurazione, completare queste operazioni. Per ulteriori informazioni, vedere Importazione delle impostazioni di configurazione personalizzate.

1. Fare clic sulla scheda **File di configurazione**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `SLES` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file delle impostazioni di configurazione da importare (ad esempio, `SLES_locale_customConfig.json`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo

   Nota: Quando si importa un file delle impostazioni di configurazione personalizzate, XClarity Administrator genera macro personalizzate per ogni impostazione nel file. È possibile aggiungere queste macro nel file di installazione automatica. Durante la distribuzione del sistema operativo, le macro vengono sostituite con i valori effettivi.

Passo 3. Modificare il file di installazione automatica di SLES per specificare i valori per le impostazioni locali del sistema operativo e della tastiera, nonché gli indirizzi IP del server NTP. Quindi importare il file personalizzato nel repository di immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione di file di installazione automatica personalizzati.

Subito dopo il tag <profile>, aggiungere le informazioni sul server NTP e la rete. Il seguente esempio include i tag per due server NTP. Gli indirizzi IP verranno aggiunti come macro in un passaggio successivo.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
   <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

Nella sezione <general>, aggiungere le informazioni sulle impostazioni locali del sistema operativo e della tastiera, come mostrato nel seguente esempio. Le impostazioni locali della tastiera e del sistema operativo verranno aggiunte come macro in un passaggio successivo.

```
<keyboard>
   <keymap></keymap>
</keyboard>
<language></language>
```

Nota: Quando si utilizza un file di installazione automatica personalizzato, XClarity Administrator non fornisce diverse funzioni utili, disponibili quando si usa un file di installazione automatica predefinito. Ad esempio, le destinazioni **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>** e **<UserAccounts>** for Administrator, **<Interfaces>** per la rete e l'elenco **<package>** per le funzioni

di installazione devono essere specificati nel file di installazione automatica personalizzato in fase di caricamento.

Per importare il file di installazione automatica personalizzato, completare la seguente procedura.

1. Fare clic sulla scheda **File di installazione automatica**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `SLES` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file di installazione automatica da importare (ad esempio, `SLES_locale_customUnattend.xml`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo

Passo 4. Associare il file di installazione automatica personalizzato con il file delle impostazioni di configurazione personalizzate e aggiungere le macro predefinite e personalizzate richieste (impostazioni) dal file delle impostazioni di configurazione al file di installazione automatica. Per ulteriori informazioni, vedere Associazione di un file di installazione automatica con un file delle impostazioni di configurazione, Inserimento di macro predefinite e personalizzate in un file di installazione automatica.

Suggerimento: è possibile utilizzare facoltativamente il file di installazione automatica personalizzato con il file delle impostazioni di configurazione personalizzato e aggiungere le macro quando si importano i file di installazione automatica.

1. Dalla scheda **File di installazione automatica**, selezionare il file di installazione automatica personalizzato (ad esempio, `SLES_locale_customUnattend.xml`).
2. Fare clic sull'icona **Associa un file di configurazione** () per visualizzare la finestra di dialogo "Associa file di installazione automatica".
3. Selezionare il file delle impostazioni di configurazione da associare al file di installazione automatica (ad esempio, `SLES_locale_customConfig`).
4. Aggiungere le macro predefinite richieste al file di installazione automatica.
   a. Selezionare **Predefinito** dall'elenco a discesa **Macro disponibili**.
   b. Posizionare il cursore in un punto qualsiasi del file di installazione automatica dopo la riga 1 (dopo il tag **<xml>**).
   c. Espandere l'elenco **predefinito → unattendSettings** nell'elenco di macro predefinite.
   d. Fare clic sulle marco **preinstallConfig** e **postinstallConfig** per aggiungere le macro.

   Ad esempio:

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

5. Aggiungere la macro personalizzata per specificare le impostazioni locali del sistema operativo.
   a. Selezionare **Personalizzato** dall'elenco a discesa **Macro disponibili**
   b. Posizionare il cursore dopo il tag **<language>**.
   c. Espandere **impostazioni-server → nodo** nell'elenco delle macro personalizzate disponibili e quindi fare clic su **impostazioni locali** per aggiungere la macro delle impostazioni locali del sistema operativo.

   Ad esempio:

```
<language>#server-settings.node.locale#</language>
```

6. Aggiungere la macro personalizzata per specificare le impostazioni locali della tastiera.
   a. Posizionare il cursore dopo il tag **<keymap>**.
   b. Espandere **impostazioni-server → nodo** nell'elenco delle macro personalizzate disponibili e quindi fare clic su **keyboardLocale** per aggiungere la macro delle impostazioni locali della tastiera.

   Ad esempio:

```
<keyboard>
   <keymap>#server-settings.node.keyboardLocale#</keymap>
</keyboard>
```

7. Aggiungere la macro personalizzata per specificare gli indirizzi IP del server NTP.

   In questo scenario, il file delle impostazioni di configurazione personalizzato utilizza un modello per specificare da nessuno a tre server NTP. Quando si utilizzano i modelli nel file delle impostazioni di configurazione, le macro associate al modello non vengono visualizzate nella finestra di dialogo "Associa file di installazione automatica". Infatti, è necessario modificare manualmente il file di installazione automatica e aggiungere macro e tag appropriati.

   Ad esempio, per includere tre server NTP, aggiungere i seguenti tag e macro al file di installazione automatica. Questi tag e macro esistono già nel file di installazione automatica di esempio per questo scenario.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address>#server-settings.ntpserver1#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address>#server-settings.ntpserver2#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address>#server-settings.ntpserver3#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
    <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

8. Fare clic su **Associa** per associare i file e salvare le modifiche nel file di installazione automatica.

Passo 5. Creare un profilo immagine del sistema operativo personalizzato che include le impostazioni di configurazione personalizzate e i file di installazione automatica. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare un profilo immagine del sistema operativo da personalizzare (ad esempio, `Basic`).

3. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio, `SLES personalizzato per impostazioni locali di sistema operativo e tastiera e server NTP`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.
   c. Selezionare **File delle impostazioni di configurazione e di installazione automatica associati** per il tipo di personalizzazione.
   d. Fare clic su **Avanti**.
5. Nella scheda **Opzioni driver** fare clic su **Avanti**. Per impostazione predefinita sono inclusi i driver di dispositivo base.
6. Nella scheda **Software** fare clic su **Avanti**.
7. Nella scheda **File di installazione automatica**, selezionare il file di installazione automatica (ad esempio, `SLES_locale_customUnattend.xml`) e fare clic su **Avanti**.

   Il file delle impostazioni di configurazione associato viene selezionato automaticamente.
8. Nella scheda **Script di installazione**, fare clic su **Avanti**.
9. Nella scheda **Riepilogo**, verificare le impostazioni.
10. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato.

Passo 6. Distribuire il profilo immagine del sistema operativo personalizzato sul server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

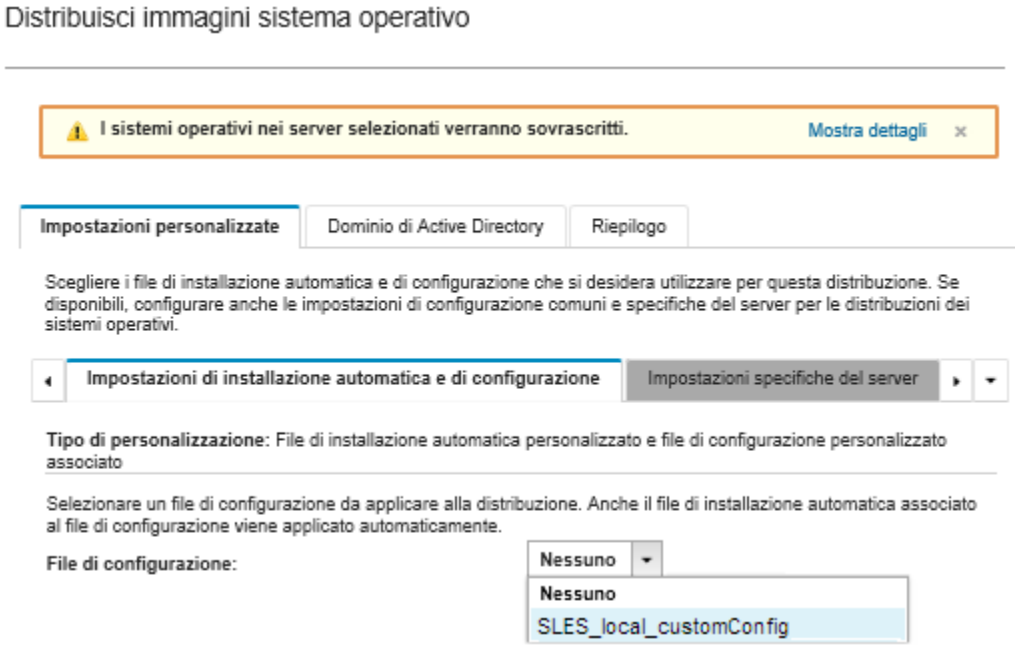
1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento: le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, <*base_OS*>|<*timestamp*>`_SLES personalizzato per impostazioni locali di sistema operativo e tastiera e server NTP`) dall'elenco a discesa nella colonna **Immagine da distribuire**.

      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.
   d. Selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.

      Nota: per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.
   e. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.
3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** ( ) per avviare la distribuzione del sistema operativo.
4. Nella scheda **Impostazioni personalizzate**, fare clic sulla scheda secondaria **Impostazioni di configurazione e di installazione automatica** e selezionare il file delle impostazioni di configurazione personalizzato (ad esempio, `SLES_locale_customConfig`).

Nota: Il file di installazione automatica personalizzato associato viene selezionato automaticamente.



5. Nella scheda secondaria **Impostazioni specifiche del server**, selezionare il server di destinazione, le impostazioni locali del sistema operativo e della tastiera.
6. Nella scheda secondaria **Impostazioni comuni**, fare clic su **Aggiungi** per specificare l'indirizzo IP di massimo tre server NTP.
7. Nella scheda **Riepilogo**, verificare le impostazioni.
8. Fare clic su **Distribuisci** per distribuire il sistema operativo.

Distribuzione di VMware ESXi v6.7 con Lenovo Customization su un disco locale utilizzando un indirizzo IP statico

In questo scenario viene installato VMware ESXi v6.7 con il sistema operativo Lenovo Customization sul disco locale, utilizzando l'indirizzo IP statico del server host. Viene utilizzato un profilo immagine del sistema operativo personalizzato che include un file di installazione automatica con le macro predefinite. Questo profilo personalizzato può essere selezionato nella pagina "Distribuisci immagini sistema operativo". I valori noti vengono sostituiti alle macro predefinite nel file di installazione automatica personalizzato e il programma di installazione Kickstart di VMware ESXi utilizza questi valori nel file di installazione automatica per configurare il sistema operativo.

Prima di iniziare

In questo scenario vengono utilizzati i seguenti file di esempio.

- ESXi_staticIP_customUnattend.cfg. Questo file di installazione automatica personalizzato utilizza i valori nelle macro predefinite.

Procedura

Per distribuire VMware ESXi v6.7 utilizzando un profilo immagine del sistema operativo personalizzato, completare le seguenti operazioni.

Passo 1. Scaricare VMware vSphere® Hypervisor (ESXi) con il sistema operativo Lenovo Customization dal sito Web Supporto VMware - Pagina Web dei download e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine ESXi da importare (ad esempio, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata.

Passo 2. Modificare il file (Kickstart) di installazione automatica di ESXi per aggiungere le macro predefinite richieste e altre macro predefinite dove applicabile, come indirizzo IP, gateway, DNS e impostazioni del nome host. Quindi importare il file personalizzato nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione di file di installazione automatica personalizzati.

Solo per ESXi e RHEL, XClarity Administrator fornisce la macro **#predefined.unattendSettings.networkConfig#** che aggiunge tutte le impostazioni di rete definite nell'interfaccia utente al file di installazione automatica. Poiché questo esempio specifica un'impostazione (**--addvmportgroup**) non definita nell'interfaccia utente, la macro .**#predefinedunattendSettings.storageConfig#** non viene utilizzata nel file di installazione automatica di esempio. Di contro, le impostazioni di rete vengono aggiunte singolarmente al file e vengono utilizzate le macro **#predefined.hostPlatforms.networkSettings.**<*setting*>**#**.

Solo per ESXi e RHEL, XClarity Administrator fornisce anche la macro **#predefined.unattendSettings.storageConfig#** che aggiunge tutte le impostazioni di storage definite nell'interfaccia utente al file di installazione automatica. Poiché questo esempio specifica le impostazioni (**--novmfsondisk** e **–ignoressd**) non definite nell'interfaccia utente, la macro **#predefinedunattendSettings.storageConfig#** non viene utilizzata nel file di installazione automatica di esempio. Di contro, le impostazioni di storage vengono aggiunte singolarmente e **--firstdisk=local** viene codificato nel file.

Nota: XClarity Administrator fornisce alcune macro di base utili, come aggiunta di driver OOB, report di stato, script post-installazione e software personalizzato. Tuttavia, per sfruttare queste macro predefinite, è necessario specificare le seguenti macro nel file di installazione automatica personalizzato. Il file di esempio contiene già le macro richieste. Tenere presente che, poiché è inclusa la sezione firstboot%, l'ordinazione di queste macro predefinite è importante. Per ulteriori informazioni, vedere Importazione di file di installazione automatica personalizzati.
`#predefined.unattendSettings.preinstallConfig#`
`#predefined.unattendSettings.postinstallConfig#`
Il file di esempio contiene già le macro richieste e le macro predefinite aggiuntive per specificare dinamicamente le impostazioni di rete per il server di destinazione. Per ulteriori informazioni sull'aggiunta di macro ai file di installazione automatica, vedere Inserimento di macro predefinite e personalizzate in un file di installazione automatica.

Per ulteriori informazioni sulle macro predefinite disponibili, vedere Macro predefinite.

Per importare il file di installazione automatica personalizzato, completare la seguente procedura.

1. Fare clic sulla scheda **File di installazione automatica**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `ESXi` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file di installazione automatica da importare (ad esempio, `ESXi_staticIP_customUnattend.cfg`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo

Passo 3. Creare un profilo immagine del sistema operativo personalizzato che include il file di installazione automatica personalizzato. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare un profilo immagine del sistema operativo da personalizzare (ad esempio, `Virtualization`).
3. Fare clic sull'icona **Crea** () per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio `ESXi personalizzato mediante l'IP statico`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.
   c. Selezionare **Solo file di installazione automatica** per il tipo di personalizzazione.
   d. Fare clic su **Avanti**.
5. Nella scheda **File di installazione automatica**, selezionare il file di installazione automatica (ad esempio, `ESXi_staticIP_customUnattend.cfg`) e fare clic su **Avanti**.
6. Nella scheda **Riepilogo**, verificare le impostazioni.
7. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato.

Passo 4. Distribuire il profilo immagine del sistema operativo personalizzato sul server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento:

      - Le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
      - Le impostazioni di rete specificate nella finestra di dialogo "Impostazioni di rete" vengono aggiunte in fase di esecuzione al file di installazione automatica, utilizzando le macro **#predefined.hostPlatforms.networkSettings.**<*setting*>**#**.

   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, <*base_OS*>|<*timestamp*>`_ESXi personalizzato mediante l'IP statico`) dall'elenco a discesa nella colonna **Immagine da distribuire**

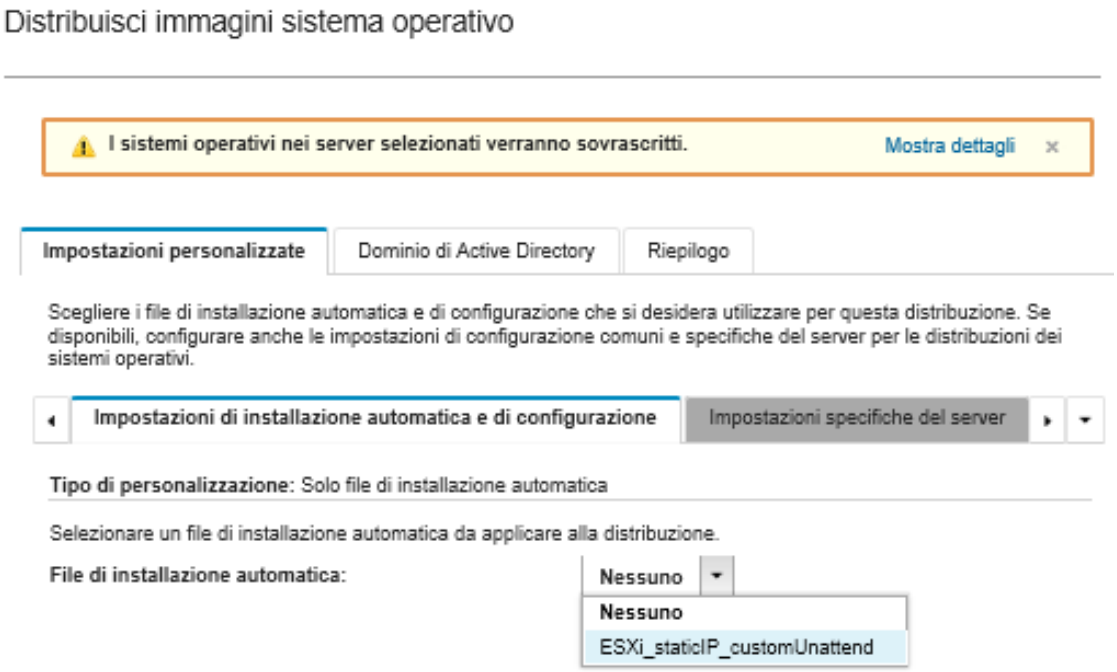
      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.

   d. (Facoltativo) Fare clic sull'icona **Chiave di licenza** () e specificare la chiave di licenza da utilizzare per attivare il sistema operativo dopo l'installazione.

e. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.

Nota: Poiché **--firstdisk=local** viene specificato nel file di installazione automatica, non è necessario specificare la posizione di storage preferita nella colonna **Storage**. L'impostazione nell'interfaccia utente viene ignorata.

3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** ( ) per avviare la distribuzione del sistema operativo.
4. Nella scheda **Impostazioni personalizzate**, fare clic sulla scheda secondaria **Impostazioni di configurazione e di installazione automatica** e selezionare il file di installazione automatica personalizzato (ad esempio, `ESXi_staticIP_customUnattend.cfg`).



5. Nella scheda **Riepilogo**, verificare le impostazioni.
6. Fare clic su **Distribuisci** per distribuire il sistema operativo.

Distribuzione di VMware ESXi v6.7 con Lenovo Customization con le impostazioni locali configurabili e le credenziali di un secondo utente

In questo scenario viene installato VMware ESXi v6.7 con il sistema operativo Lenovo Customization con una lingua configurabile abilitata per le impostazioni locali della tastiera e le credenziali per un secondo utente ESXi. In questo esempio vengono utilizzate anche le impostazioni di base di rete e storage definite nell'interfaccia utente. Viene utilizzato un profilo immagine sistema operativo personalizzato che include un file di installazione automatica (con macro predefinite e personalizzate) e un file delle impostazioni di configurazione per selezionare la password. Questo profilo personalizzato può essere selezionato nella pagina "Distribuisci immagini sistema operativo". Quindi, è possibile specificare la password nella scheda **Impostazioni personalizzate**. Il valore selezionato viene sostituito alla macro personalizzata nel file di installazione automatica personalizzato e il programma di installazione di ESXi utilizza questi valori per configurare il sistema operativo.

Prima di iniziare

In questo scenario vengono utilizzati i seguenti file di esempio.

- ESXi_locale_customConfig.json. Questo file di configurazione personalizzato richiede per le impostazioni locali della tastiera e le credenziali per il secondo utente ESXi.
- ESXi_locale_customUnattend.cfg. Questo file di installazione automatica personalizzato utilizza i valori nelle macro predefinite e personalizzate definiti nel file di configurazione.

Procedura

Per distribuire VMware ESXi v6.7 utilizzando un profilo immagine del sistema operativo personalizzato, completare le seguenti operazioni.

Passo 1. Scaricare VMware vSphere® Hypervisor (ESXi) con il sistema operativo Lenovo Customization dal sito Web Supporto VMware - Pagina Web dei download e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine ESXi da importare (ad esempio, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata.

Passo 2. Creare un file delle impostazioni di configurazione personalizzate e importarlo nel repository di immagini del sistema operativo.

Il file delle impostazioni di configurazione è un file JSON che descrive i dati che devono essere raccolti dinamicamente durante il processo di distribuzione del sistema operativo. Per questo scenario, si desidera scegliere impostazioni locali della tastiera, l'ID utente e la password per un secondo utente ESXi, da utilizzare per ciascuna distribuzione del sistema operativo. Per ulteriori informazioni sulla creazione di un file delle impostazioni di configurazione, vedere Macro personalizzate.

Per importare il file delle impostazioni di configurazione, completare queste operazioni. Per ulteriori informazioni, vedere Importazione delle impostazioni di configurazione personalizzate.

1. Fare clic sulla scheda **File di configurazione**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `ESXi` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file delle impostazioni di configurazione da importare (ad esempio, `ESXi_locale_customConfig.json`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo

   Nota: Quando si importa un file delle impostazioni di configurazione personalizzate, XClarity Administrator genera macro personalizzate per ogni impostazione nel file. È possibile aggiungere queste macro nel file di installazione automatica. Durante la distribuzione del sistema operativo, le macro vengono sostituite con i valori effettivi.

Passo 3. Modificare il file (Kickstart) di installazione automatica di ESXi per specificare i valori per le impostazioni locali del sistema operativo e della tastiera, nonché le credenziali utente per il

secondo utente ESXi. Quindi importare il file personalizzato nel repository di immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione di file di installazione automatica personalizzati.

Aggiungere i comandi per configurare le impostazioni locali della tastiera, ad esempio:

```
# Set the keyboard locale
keyboard ''
```

Aggiungere i comandi per creare un secondo utente ESXi. Nel seguente esempio, *<user_id>* e *<password>* verranno sostituiti con macro personalizzate nel passaggio successivo.

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp <user_id>
echo <password> | /usr/lib/vmware/auth/bin/passwd <user_id> --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root <user_id> false Admin true
```

Per importare il file di installazione automatica personalizzato, completare la seguente procedura.

1. Fare clic sulla scheda **File di installazione automatica**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `ESXi` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file di installazione automatica da importare (ad esempio, `ESXi_locale_customUnattend.cfg`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo

Passo 4. Associare il file di installazione automatica personalizzato con il file delle impostazioni di configurazione personalizzate e aggiungere le macro predefinite e personalizzate richieste (impostazioni) dal file delle impostazioni di configurazione al file di installazione automatica. Per ulteriori informazioni, vedere Associazione di un file di installazione automatica con un file delle impostazioni di configurazione, Inserimento di macro predefinite e personalizzate in un file di installazione automatica.

Suggerimento:

- È possibile associare facoltativamente il file di installazione automatica personalizzato con il file delle impostazioni di configurazione personalizzato e aggiungere le macro quando si importano i file di installazione automatica.
- XClarity Administrator fornisce alcune macro di base utili, come aggiunta di driver OOB, report di stato, script post-installazione e software personalizzato. Tuttavia, per sfruttare queste macro predefinite, è necessario specificare le seguenti macro nel file di installazione automatica personalizzato. Il file di esempio contiene già le macro richieste. Tenere presente che, poiché è inclusa la sezione firstboot%, l'ordinazione di queste macro predefinite è importante. Per ulteriori informazioni, vedere Importazione di file di installazione automatica personalizzati.

  ```
  #predefined.unattendSettings.preinstallConfig#
  #predefined.unattendSettings.postinstallConfig#
  ```

- XClarity Administrator fornisce anche macro che inseriscono tutte le impostazioni sulla posizione di storage e rete, definite nell'interfaccia utente. Queste macro sono utili quando per la distribuzione sono necessarie solo le impostazioni di base. Il file di esempio contiene già le macro richieste.

  ```
  #predefined.unattendSettings.networkConfig#
  #predefined.unattendSettings.storageConfig#
  ```

Per ulteriori informazioni sull'aggiunta di macro ai file di installazione automatica, vedere Inserimento di macro predefinite e personalizzate in un file di installazione automatica. Per ulteriori informazioni sulle macro predefinite disponibili, vedere Macro predefinite.

Per associare il file di installazione automatica personalizzato al file delle impostazioni di configurazione personalizzate, completare la seguente procedura.

1. Dalla scheda **File di installazione automatica**, selezionare il file di installazione automatica personalizzato (ad esempio, `ESXi_locale_customUnattend.cfg`).
2. Fare clic sull'icona **Associa un file di configurazione** () per visualizzare la finestra di dialogo "Associa file di installazione automatica".
3. Selezionare il file delle impostazioni di configurazione da associare al file di installazione automatica (ad esempio, `ESXi_locale_customConfig`).
4. Selezionare **Personalizzato** dall'elenco a discesa **Macro disponibili**.
5. Aggiungere la macro personalizzata per specificare le impostazioni locali della tastiera, posizionando il cursore tra le virgolette singole dopo la tastiera. Quindi fare clic su **keyboard_locale**.

   Ad esempio:

   ```
   # Set the keyboard locale
   keyboard '#keyboard_locale#'
   ```

6. Aggiungere la macro personalizzata per specificare l'ID del secondo utente, posizionando il cursore in ciascuna posizione dove si desidera aggiungere l'ID utente. Quindi fare clic su **second_user_id**. Nel file di esempio, sostituire ogni occorrenza di *<user_id>* con la macro personalizzata.

   Ad esempio:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo <password> | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

7. Aggiungere la macro personalizzata per specificare la password del secondo utente, posizionando il cursore nella posizione dove si desidera aggiungere la password. Quindi fare clic su **second_user_password**. Nel file di esempio, sostituire *<password>* con la macro personalizzata.

   Ad esempio:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo #second_user_password# | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

8. Fare clic su **Associa** per associare i file e salvare le modifiche nel file di installazione automatica.

Passo 5. Creare un profilo immagine del sistema operativo personalizzato che include le impostazioni di configurazione personalizzate e i file di installazione automatica. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare un profilo immagine del sistema operativo da personalizzare (ad esempio, `Virtualization`).
3. Fare clic sull'icona **Crea** () per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio, `ESXi personalizzato mediante le impostazioni locali personalizzate e le credenziali del secondo utente`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.

c. Selezionare **File delle impostazioni di configurazione e di installazione automatica associati** per il tipo di personalizzazione.
d. Fare clic su **Avanti**.

5. Nella scheda **File di installazione automatica**, selezionare il file di installazione automatica (ad esempio, `ESXi_locale_customUnattend.cfg`) e fare clic su **Avanti**.

   Il file delle impostazioni di configurazione associato viene selezionato automaticamente.

6. Nella scheda **Riepilogo**, verificare le impostazioni.
7. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato.

Passo 6. Distribuire il profilo immagine del sistema operativo personalizzato sul server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento:

      - Le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
      - Le impostazioni di rete specificate nella finestra di dialogo "Impostazioni di rete" vengono aggiunte in fase di esecuzione al file di installazione automatica, utilizzando la macro **#predefined.hostPlatforms.networkConfig#**.

   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, <*base_OS*>|<*timestamp*>`_ESXi personalizzato mediante le impostazioni locali personalizzate e le credenziali del secondo utente`) dall'elenco a discesa nella colonna **Immagine da distribuire**

      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.

   d. (Facoltativo) Fare clic sull'icona **Chiave di licenza** () e specificare la chiave di licenza da utilizzare per attivare il sistema operativo dopo l'installazione.
   e. Selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.

      Nota:

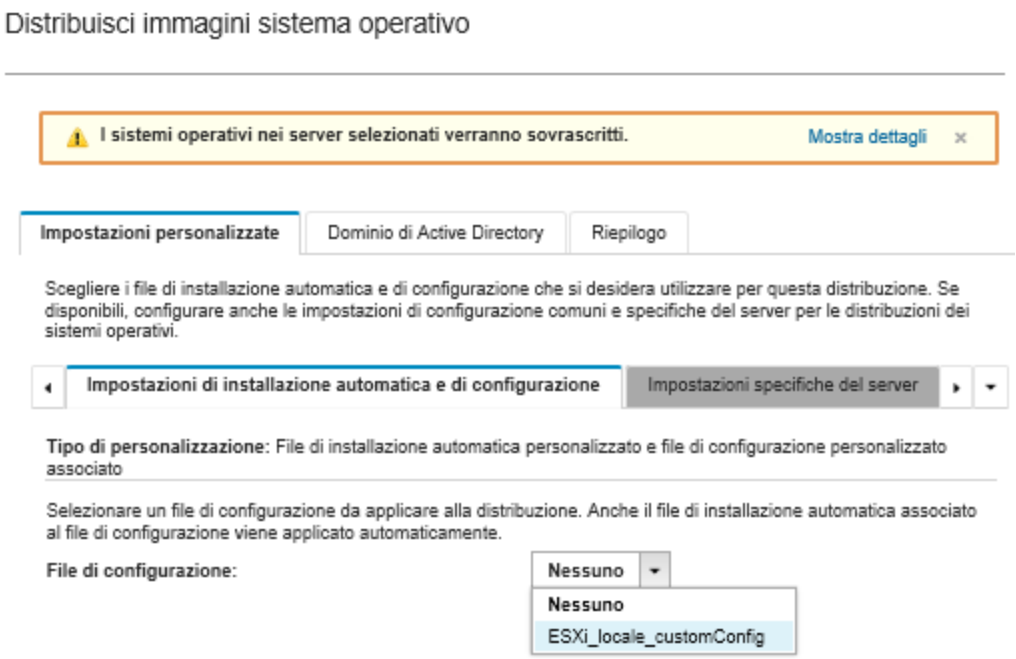
      - per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.
      - Le impostazioni di storage specificate nella finestra di dialogo "Impostazioni di storage" vengono aggiunte in fase di esecuzione al file di installazione automatica, utilizzando la macro **#predefined.hostPlatforms.storageConfig#**.

   f. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.

3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** () per avviare la distribuzione del sistema operativo.

4. Nella scheda **Impostazioni personalizzate**, fare clic sulla scheda secondaria **Impostazioni di configurazione e di installazione automatica** e selezionare il file delle impostazioni di configurazione personalizzato (ad esempio, `ESXi_locale_customConfig`).

   Nota: Il file di installazione automatica personalizzato associato viene selezionato automaticamente.

5. Nella scheda secondaria **Impostazioni specifiche del server**, selezionare le impostazioni locali della tastiera e le credenziali per il secondo utente ESXi.
6. Nella scheda **Riepilogo**, verificare le impostazioni.
7. Fare clic su **Distribuisci** per distribuire il sistema operativo.

Distribuzione di Windows 2016 con funzioni personalizzate

In questo scenario vengono installati il sistema operativo Windows 2016 e diverse funzioni aggiuntive. Viene utilizzato un profilo personalizzato che include un file di installazione automatica personalizzato. Il profilo personalizzato può quindi essere selezionato nella pagina "Distribuisci immagini sistema operativo".

Prima di iniziare

In questo scenario vengono utilizzati i seguenti file di esempio.

- Windows_installFeatures_customUnattend.xml. Questo file di installazione automatica personalizzato installa le funzioni WindowsMediaPlayer e BitLocker e utilizza le macro predefinite per i valori dinamici.

Procedura

Per distribuire Windows 2016 con funzioni personalizzate, completare la seguente procedura.

Passo 1. Scaricare il sistema operativo Windows 2016 in giapponese nel sistema locale e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

   1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.

2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine del sistema operativo che si desidera importare (ad esempio, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 2. Scaricare il file del bundle per Windows 2016 nel sistema locale e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione dei driver di dispositivo.

Il file del bundle contiene i driver di dispositivo più recenti e i file di avvio WinPE che è possibile aggiungere ai profili personalizzati di immagini del sistema operativo. In questo scenario utilizza un file di avvio personalizzato, in modo che il file di avvio nel bundle non venga utilizzato.

1. Fare clic sulla scheda **File del driver**.
2. Fare clic su **Scarica → File del bundle di Windows** per accedere alla pagina Web del supporto Lenovo e scaricare il file del bundle per Windows 2016 nel sistema locale.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine del sistema operativo da importare (ad esempio, `bundle_win2016_20180126130051.zip`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 3. Modificare il file di installazione automatica di Windows per installare le funzioni aggiuntive (come WindowsMediaPlayer e BitLocker) e importare il file personalizzato nel repository delle immagini del sistema operativo.

Nella sezione "manutenzione" del file di installazione automatica di Windows, aggiungere le funzionalità di Windows da installare, ad esempio

```
<servicing>
   <package action="configure">
      <assemblyIdentity name="Microsoft-Windows-Foundation-Package" version="10.0.14393.0"
                        processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
                        language=""></assemblyIdentity>
      <selection name="Microsoft-Hyper-V" state="true"></selection>
      <selection name="MultipathIo" state="true"></selection>
      <selection name="FailoverCluster-PowerShell" state="true"></selection>
      <selection name="FailoverCluster-FullServer" state="true"></selection>
      <selection name="FailoverCluster-CmdInterface" state="true"></selection>
      <selection name="FailoverCluster-AutomationServer" state="true"></selection>
      <selection name="FailoverCluster-AdminPak" state="true"></selection>
      <selection name="MicrosoftWindowsPowerShellRoot" state="true"></selection>
      <selection name="MicrosoftWindowsPowerShell" state="true"></selection>
      <selection name="ServerManager-Core-RSAT" state="true"></selection>
      <selection name="WindowsMediaPlayer" state="true"></selection>
      <selection name="BitLocker" state="true"></selection>
   </package>
</servicing>
```

Nota:

- Questi tag sono nel file di installazione automatica di esempio.

- Quando si utilizza un file di installazione automatica personalizzato, XClarity Administrator non fornisce diverse funzioni utili, disponibili quando si usa un file di installazione automatica predefinito. Ad esempio, le destinazioni `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>` e `<UserAccounts>` per l'amministratore, `<Interfaces>` per la rete e l'elenco `<package>` per le funzionalità di installazione devono essere specificati nel file di installazione automatica personalizzato in fase di caricamento.

Per importare il file di installazione automatica personalizzato, completare la seguente procedura. Per ulteriori informazioni, vedere Importazione di file di installazione automatica personalizzati.

1. Fare clic sulla scheda **File di installazione automatica**.
2. Fare clic sull'icona **Importa** ( ).
3. Fare clic su **Importazione locale**.
4. Selezionare `Windows` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file di installazione automatica personalizzato (ad esempio, `Windows_installFeatures_customUnattend.xml`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

XClarity Administrator fornisce alcune utili macro di base, come aggiunta di driver OOB, report di stato, script post-installazione e software personalizzato. Tuttavia, per sfruttare queste macro predefinite, è necessario specificare le seguenti macro nel file di installazione automatica personalizzato.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

Il file di esempio contiene già il codice per l'installazione delle funzioni aggiuntive, le macro richieste e altre macro necessarie per l'immissione dinamica. Per ulteriori informazioni sull'aggiunta di macro ai file di installazione automatica, vedere Inserimento di macro predefinite e personalizzate in un file di installazione automatica.

Per ulteriori informazioni sulle macro predefinite disponibili, vedere Macro predefinite.

Passo 4. Creare un profilo immagine del sistema operativo personalizzato che include il file di installazione automatica. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare il profilo da personalizzare (ad esempio, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio `Windows personalizzato con funzioni`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.
   c. Selezionare **Solo file di installazione automatica** per il tipo di personalizzazione.
   d. Fare clic su **Avanti**.
5. Nella scheda **Opzioni driver** fare clic su **Avanti**. Per impostazione predefinita sono inclusi i driver di dispositivo base.
6. Nella scheda **Opzioni di avvio** fare clic su **Avanti**. Il file di avvio WinPE predefinito viene selezionato per impostazione predefinita.
7. Nella scheda **Software** fare clic su **Avanti**.

8. Nella scheda **File di installazione automatica**, selezionare il file di installazione automatica personalizzato (ad esempio, `Windows_installFeatures_customUnattend.xml`) e fare clic su **Avanti**.
9. Nella scheda **Script di installazione**, fare clic su **Avanti**.
10. Nella scheda **Riepilogo**, verificare le impostazioni.
11. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato

Passo 5. Distribuire il profilo immagine del sistema operativo personalizzato ai server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP, la maschera di sottorete, il gateway e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento: le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, *<base_OS>*|*<timestamp>*`_Windows personalizzato con funzioni`) dall'elenco a discesa nella colonna **Immagine da distribuire**.

      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.
   d. (Facoltativo) Fare clic sull'icona **Chiave di licenza** () e specificare la chiave di licenza da utilizzare per attivare il sistema operativo dopo l'installazione.
   e. Selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.

      Nota: Per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo
   f. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.
3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** () per avviare la distribuzione del sistema operativo.
4. Nella scheda **Impostazioni personalizzate**, fare clic sulla scheda secondaria **Impostazioni di configurazione e di installazione automatica** e selezionare il file di installazione automatica personalizzato (ad esempio, `Windows_installFeatures_customUnattend.xml`).
5. (Facoltativo) Nella scheda **Dominio di Active Directory**, specificare le informazioni per unire un dominio di Active Directory nell'ambito della distribuzione dell'immagine di Windows (vedere Integrazione con Windows Active Directory).
6. Nella scheda **Riepilogo**, verificare le impostazioni.
7. Fare clic su **Distribuisci** per distribuire il sistema operativo.

Distribuzione di Windows 2016 con software personalizzato

In questo scenario viene installato il sistema operativo Windows 2016 con software personalizzato (Java ed Eclipse IDE). Viene utilizzato un profilo personalizzato che include il software personalizzato e gli script post-installazione per installare e configurare il software personalizzato. I pacchetti software personalizzati

vengono copiati sull'host durante la distribuzione e possono essere utilizzati per lo script post-installazione personalizzato.

Prima di iniziare

In questo scenario vengono utilizzati i seguenti file di esempio.

- jre-8u151-windows-x64-with-configfile.zip. Questo è il file di installazione di Java per Eclipse.
- eclipse-java-oxygen-1a-win32-x86_64.zip Questo è il file di installazione di Eclipse IDE.
- Windows_installSoftware_customScript.ps1 Questo script post-installazione crea un utente per avviare Eclipse e installa Eclipse IDE e Java.

Nota:

- Gli script di installazione di Windows sono disponibili in uno dei seguenti formati: File di comando (.cmd), PowerShell (.ps1)
- I file dei software e gli script di installazione vengono installati dal percorso dei file e dei dati personalizzati specificato durante la distribuzione. Il percorso predefinito di file e dati personalizzati è `C:\lxca`.

Procedura

Per distribuire Windows 2016 con software personalizzato, completare la seguente procedura.

Passo 1. Scaricare il sistema operativo Windows 2016 in giapponese nel sistema locale e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine del sistema operativo che si desidera importare (ad esempio, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 2. Scaricare il file del bundle per Windows 2016 nel sistema locale e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione dei driver di dispositivo.

Il file del bundle contiene i driver di dispositivo più recenti e i file di avvio WinPE che è possibile aggiungere ai profili personalizzati di immagini del sistema operativo. In questo scenario utilizza un file di avvio personalizzato, in modo che il file di avvio nel bundle non venga utilizzato.

1. Fare clic sulla scheda **File del driver**.
2. Fare clic su **Scarica → File del bundle di Windows** per accedere alla pagina Web del supporto Lenovo e scaricare il file del bundle per Windows 2016 nel sistema locale.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine del sistema operativo da importare (ad esempio, `bundle_win2016_20180126130051.zip`).

6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 3. Scaricare il software personalizzato nel sistema locale e importare i file nel repository di immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione di software personalizzato.

1. Fare clic sulla scheda **Software**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `Windows` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file delle impostazioni di configurazione da importare (ad esempio, `jre-8u151-windows-x64-with-configfile.zip`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.
7. Fare clic nuovamente sull'icona **Importa** ().
8. Fare clic su **Importazione locale**.
9. Selezionare `Windows` per il sistema operativo.
10. Fare clic su **Sfoglia** per individuare e selezionare il file delle impostazioni di configurazione da importare (ad esempio, `eclipse-java-oxygen-1a-win32-x86_64.zip`).
11. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

Passo 4. Creare uno script di post-installazione personalizzato e importare il file nel repository di immagini del sistema operativo.

Aggiungere i comandi per installare il software, ad esempio:

```
Write-Output "Install Java...."
Invoke-Command -ScriptBlock
        {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
        [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg]
        /s}

Write-Output "Install Eclipse..."
$eclipseDir="C:\Users\Administrator\Desktop\eclipse"
New-Item -ItemType directory -Path $eclipseDir
Expand-Archive -LiteralPath
        "#predefined.otherSettings.deployDataAndSoftwareLocation#\eclipse-java-oxygen-1a-win32-x86_64.zip"
        -DestinationPath $eclipseDir
```

Tenere presente che questi comandi utilizzano la macro predefinita per il percorso dei dati estratti e i file del software (**predefined.otherSettings.deployDataAndSoftwareLocation**).

È anche possibile aggiungere i comandi per inviare messaggi personalizzati al log dei processi inXClarity Administrator, come mostrato nel file di esempio. Per ulteriori informazioni, vedere Aggiunta di report di stato personalizzato agli script di installazione.

Per importare lo script di installazione personalizzato, completare la seguente procedura. Per ulteriori informazioni, vedere Importazione di script di installazione personalizzati.

1. Fare clic sulla scheda **Script di installazione**.
2. Fare clic sull'icona **Importa** ().
3. Fare clic su **Importazione locale**.
4. Selezionare `Windows` per il sistema operativo.

5. Fare clic su **Sfoglia** per individuare e selezionare il file di installazione automatica da importare (ad esempio, `Windows_installSoftware_customScript.ps1`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

Passo 5. Creare un profilo immagine del sistema operativo personalizzato che include il file di installazione automatica personalizzato. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare un profilo immagine del sistema operativo da personalizzare (ad esempio, `Datacenter virtualization`).
3. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio `Windows personalizzato con software`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.
   c. Selezionare **Nessuno** per il tipo di personalizzazione.
   d. Fare clic su **Avanti**.
5. Nella scheda **Opzioni driver** fare clic su **Avanti**. Per impostazione predefinita sono inclusi i driver di dispositivo base.
6. Nella scheda **Opzioni di avvio** fare clic su **Avanti**. Il file di avvio WinPE predefinito viene selezionato per impostazione predefinita.
7. Nella scheda **Software**, selezionare i file di installazione del software (ad esempio, `jre-8u151-windows-x64-with-configfile.zip` e `eclipse-java-oxygen-1a-win32-x86_64.zip`) e fare clic su **Avanti**.
8. Nella scheda **Script di installazione**, selezionare gli script di installazione (ad esempio, `Windows_installSoftware_customScript.ps1`) e fare clic su **Avanti**.
9. Nella scheda **Riepilogo**, verificare le impostazioni.
10. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato.

Passo 6. Distribuire il profilo immagine del sistema operativo personalizzato ai server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento: le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, *<base_OS>*|*<timestamp>*`_Windows personalizzato con software`) dall'elenco a discesa nella colonna **Immagine da distribuire**.

      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.
   d. (Facoltativo) Fare clic sull'icona **Chiave di licenza** ( ) e specificare la chiave di licenza da utilizzare per attivare il sistema operativo dopo l'installazione.
   e. Selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.

Nota: Per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.

f. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.

3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** () per avviare la distribuzione del sistema operativo.
4. Nella scheda **Riepilogo**, verificare le impostazioni.
5. Fare clic su **Distribuisci** per distribuire il sistema operativo.

Distribuzione di Windows 2016 in giapponese

In questo scenario viene installato il sistema operativo Windows 2016 su più server in giapponese per la tastiera e le impostazioni locali del sistema operativo. Viene utilizzato un profilo personalizzato che include un file di avvio di WinPE e un file di installazione automatica. Il profilo personalizzato può quindi essere selezionato nella pagina "Distribuisci immagini sistema operativo".

Prima di iniziare

In questo scenario vengono utilizzati i seguenti file di esempio.

- `WinPE_64_ja.zip`. Questo file di avvio personalizzato di Windows (WinPE) installa le impostazioni locali giapponesi.
- Windows_locale_customUnattend.xml. Questo file di installazione automatica personalizzato utilizza il file WinPE per installare il giapponese.

Nota: Il file di installazione automatica personalizzato di esempio presuppone quanto segue:

- Il server dispone di un solo disco visibile (disco 0) privo di partizione di sistema.
- Viene utilizzata la modalità statica IPv4 che imposta un indirizzo IP statico (utilizzato nel file di installazione automatica personalizzato come macro predefinita).

Procedura

Per distribuire Windows 2016 in giapponese sui server di destinazione mediante un profilo immagine del sistema operativo personalizzato, completare le seguenti operazioni.

Passo 1. Scaricare il sistema operativo Windows 2016 in giapponese nel sistema locale e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione delle immagini del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Gestisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: Gestisci immagini sistema operativo.
2. Fare clic sulla scheda **Immagini sistema operativo**.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine del sistema operativo che si desidera importare (ad esempio, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Fare clic su **Importa** per caricare l'immagine nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 2. Scaricare il file del bundle per Windows 2016 nel sistema locale e importare l'immagine nel repository delle immagini del sistema operativo. Per ulteriori informazioni, vedere Importazione dei driver di dispositivo.

Il file del bundle contiene i driver di dispositivo più recenti e i file di avvio WinPE che è possibile aggiungere ai profili personalizzati di immagini del sistema operativo. In questo scenario utilizza un file di avvio personalizzato, in modo che il file di avvio nel bundle non venga utilizzato.

1. Fare clic sulla scheda **File del driver**.
2. Fare clic su **Scarica → File del bundle di Windows** per accedere alla pagina Web del supporto Lenovo e scaricare il file del bundle per Windows 2016 nel sistema locale.
3. Fare clic sull'icona **Importa** ().
4. Fare clic su **Importazione locale**.
5. Fare clic su **Sfoglia** per individuare e selezionare l'immagine del sistema operativo da importare (ad esempio, `bundle_win2016_20180126130051.zip`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.
7. Attendere che l'importazione venga completata. Ciò potrebbe richiedere tempo.

Passo 3. Creare un file di avvio WinPE personalizzato che utilizza le impostazioni locali giapponesi durante l'installazione di WinPE e importarlo nel repository delle immagini del sistema operativo.

XClarity Administrator utilizza un file di avvio predefinito di WinPE (Windows PreInstallation) per installare il sistema operativo Windows. Le impostazioni locali utilizzate con questo file di avvio predefinito sono configurate su Inglese (en-US). Se si desidera modificare le impostazioni locali utilizzate durante la configurazione di Windows, è possibile creare un file di avvio personalizzato di WinPE con le impostazioni locali desiderate e assegnare il file di avvio personalizzato al profilo personalizzato.

Per informazioni sull'inserimento delle impostazioni locali in WinPE, vedere Windows WinPE: pagina Web di aggiunta dei pacchetti.

Importante: Specificare una lingua diversa dall'inglese nelle impostazioni locali del file di avvio di WinPE non modifica le impostazioni locali del sistema operativo finale in fase di distribuzione. Vengono modificate infatti solo le impostazioni locali visualizzate durante l'installazione e la configurazione di Windows.

Per creare un file di avvio WinPE personalizzato che include le impostazioni locali giapponese, completare queste operazioni. Per ulteriori informazioni, vedere Creazione di un file di avvio (WinPE).

1. Utilizzando un ID utente con autorità di amministratore, eseguire il comando di Windows ADK "Deployment and Imaging Tools Environment". Verrà visualizzata una sessione del comando.
2. Dalla sessione del comando passare alla directory in cui i file `genimage.cmd` e `starnet.cmd` sono stati scaricati (ad esempio, `C:\customwim`).
3. Verificare che nell'host non siano presenti immagini precedentemente montate eseguendo il comando seguente:
   ```
   dism /get-mountedwiminfo
   ```
   Se sono presenti immagini montate, rimuoverle eseguendo il comando seguente:
   ```
   dism /unmount-wim /MountDir:C:\<mount_path> /Discard
   ```
4. Se si aggiungono driver di dispositivo inclusi a un profilo Windows personalizzato, copiare i file dei driver di dispositivo non elaborati, in formato .inf, nella directory `C:\drivers` del sistema host.

5. Eseguire il comando seguente per generare il file di avvio, in formato .wim, e attendere per alcuni minuti il completamento del comando.
   `genimage.cmd amd64 <ADK_Version>`

   Dove *<ADK_Version>* è uno dei seguenti valori.

   - **8.1**. Per Windows 2012 R2
   - **10**. Per Windows 2016

   Questo comando crea un file di avvio denominato `C:\WinPE_64\media\Boot\WinPE_64.wim`.
6. Montare il file di avvio eseguendo il comando seguente:
   `DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount`
7. Se si aggiungono i driver di dispositivo non inclusi direttamente al file di avvio, attenersi alla procedura descritta di seguito.
   a. Creare la seguente struttura di directory, dove *<os_release>* è `2012R2` o `2016`
      `drivers\<os_release>\`
   b. Copiare i driver di dispositivo, in formato .inf, in una directory all'interno di tale percorso, ad esempio:
      `drivers\<os_release>\<driver1>\<driver1_files>`
   c. Copiare la directory `drivers` nella directory di montaggio, ad esempio:
      `C:\WinPE_64\mount\drivers`
8. **Facoltativo:** apportare ulteriori personalizzazioni al file delle opzioni di avvio, come l'aggiunta di cartelle, file, script di avvio, language pack e applicazioni. Per ulteriori informazioni sulla personalizzazione dei file di avvio, vedere WinPE: sito Web sul montaggio e la personalizzazione.
9. Ad esempio, aggiungere i pacchetti in giapponese.
10. Visualizzare i pacchetti installati per verificare che siano stati installati specifici pacchetti in giapponese.
```
Dism /Add-Package /Image:"C:\WinPE_64\mount"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment
and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\ja-jp\lp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-DismCmdlets_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-NetFx_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-PowerShell_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-RNDIS_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-Scripting_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-StorageWMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WDS-Tools_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\WinPE-FontSupport-JA-JP.cab"
```
11. Verificare le impostazioni internazionali nell'immagine.
    `Dism /Get-Packages /Image:"C:\WinPE_64\mount"`
12. Smontare l'immagine eseguendo il comando seguente.
    `DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit`
13. Comprimere il contenuto della directory `C:\WinPE_64\media` in un file zip denominato `WinPE_64_ja.zip`.

14. Importare il file .zip in XClarity Administrator (vedere Importazione dei file di avvio).
    a. Fare clic sulla scheda **File di avvio**.
    b. Fare clic sull'icona **Importa** ().
    c. Fare clic su **Importazione locale**.
    d. Selezionare `Windows` per il sistema operativo.
    e. Fare clic su **Sfoglia** per individuare e selezionare il file di avvio personalizzato (ad esempio, `WinPE_64_ja.zip`).
    f. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

Passo 4. Modificare il file di installazione automatica di Windows per specificare che il giapponese è incluso nell'immagine del sistema operativo e importare il file personalizzato nel repository delle immagini del sistema operativo.

Nel passaggio "windowsPE" dell'installazione di Windows, aggiungere il giapponese come lingua del sistema operativo e le impostazioni locali, ad esempio:

```
<settings pass="windowsPE">
   <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64"
              publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
              xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <SetupUILanguage>
         <UILanguage>ja-JP</UILanguage>
      </SetupUILanguage>
      <SystemLocale>ja-JP</SystemLocale>
      <UILanguage>ja-JP</UILanguage>
      <UserLocale>ja-JP</UserLocale>
      <InputLocale>0411:00000411</InputLocale>
   </component>
</settings>
```

Nota: Quando si utilizza un file di installazione automatica personalizzato, XClarity Administrator non fornisce diverse funzioni utili, disponibili quando si usa un file di installazione automatica predefinito. Ad esempio, le destinazioni `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>` e `<UserAccounts>` per l'amministratore, `<Interfaces>` per la rete e l'elenco `<package>` per le funzionalità di installazione devono essere specificati nel file di installazione automatica personalizzato in fase di caricamento.

XClarity Administrator fornisce alcune macro di base utili, come aggiunta di driver OOB, report di stato, script post-installazione e software personalizzato. Tuttavia, per sfruttare queste macro predefinite, è necessario specificare le seguenti macro nel file di installazione automatica personalizzato.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

Il file di esempio contiene già le macro richieste. Per ulteriori informazioni sull'aggiunta di macro ai file di installazione automatica, vedere Inserimento di macro predefinite e personalizzate in un file di installazione automatica. Per ulteriori informazioni sulle macro predefinite disponibili, vedere Macro predefinite.

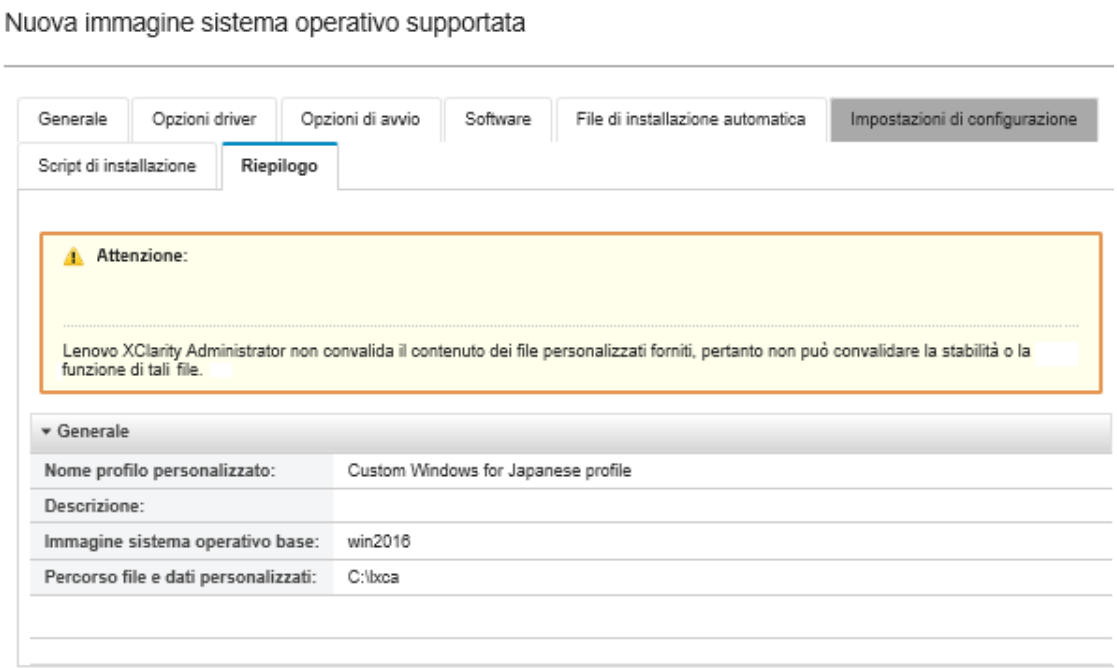
Per importare il file di installazione automatica personalizzato, completare la seguente procedura. Per ulteriori informazioni, vedere Importazione di file di installazione automatica personalizzati.

1. Fare clic sulla scheda **File di installazione automatica**.
2. Fare clic sull'icona **Importa** ().

3. Fare clic su **Importazione locale**.
4. Selezionare `Windows` per il sistema operativo.
5. Fare clic su **Sfoglia** per individuare e selezionare il file di installazione automatica personalizzato (ad esempio, `Windows_locale_customUnattend.xml`).
6. Fare clic su **Importa** per caricare il file nel repository di immagini del sistema operativo.

Passo 5. Creare un profilo immagine del sistema operativo personalizzato che include il file di avvio personalizzato (WinPE) e il file di installazione automatica. Per ulteriori informazioni, vedere Creazione di un profilo immagine del sistema operativo personalizzato.

1. Fare clic sulla scheda **Immagini sistema operativo**.
2. Selezionare il profilo da personalizzare (ad esempio, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Fare clic sull'icona **Crea** ( ) per visualizzare la finestra di dialogo "Crea profilo personalizzato".
4. Nella scheda **Generale**:
   a. Immettere un nome per il profilo (ad esempio `Profilo Windows personalizzato per il giapponese`).
   b. Utilizzare il valore predefinito per il campo **Percorso file e dati personalizzati**.
   c. Selezionare **Solo file di installazione automatica** per il tipo di personalizzazione.
   d. Fare clic su **Avanti**.
5. Nella scheda **Opzioni driver** fare clic su **Avanti**. Per impostazione predefinita sono inclusi i driver di dispositivo base.
6. Nella scheda **File di avvio**, selezionare il file di avvio personalizzato (ad esempio, `WinPE_64_ja`) e fare clic su **Avanti**.
7. Nella scheda **Software** fare clic su **Avanti**.
8. Nella scheda **File di installazione automatica**, selezionare il file di installazione automatica personalizzato (ad esempio, `Windows_locale_customUnattend.xml`) e fare clic su **Avanti**.
9. Nella scheda **Script di installazione**, fare clic su **Avanti**.
10. Nella scheda **Riepilogo**, verificare le impostazioni.



11. Fare clic su **Personalizza** per creare il profilo immagine del sistema operativo personalizzato.

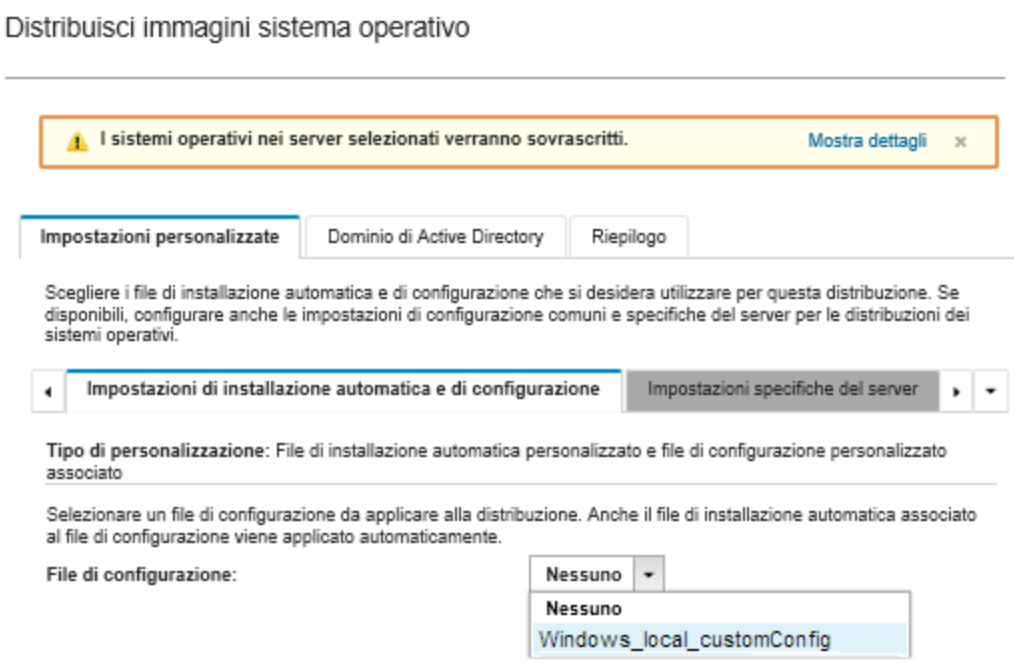
Passo 6. Distribuire il profilo immagine del sistema operativo personalizzato ai server di destinazione. Per ulteriori informazioni, vedere Distribuzione di un'immagine del sistema operativo.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo** per visualizzare la pagina Distribuisci sistema operativo: distribuisci immagini sistema operativo.
2. Per ciascun server di destinazione:
   a. Selezionare il server.
   b. Fare clic su **Modifica elementi selezionati → Impostazioni di rete** e specificare il nome host, l'indirizzo IP, la maschera di sottorete, il gateway e le impostazioni di DNS, MTU e VLAN per il server.

      Suggerimento: le impostazioni VLAN sono disponibili solo quando la modalità VLAN è impostata su **Impostazioni globali → Assegnazione IP → Usa VLAN**.
   c. Selezionare il profilo immagine del sistema operativo personalizzato (ad esempio, <*base_OS*>|<*timestamp*>_`Profilo Windows personalizzato per il giapponese`) dall'elenco a discesa nella colonna **Immagine da distribuire**.

      Nota: Verificare che tutti i server di destinazione utilizzino lo stesso profilo personalizzato.
   d. (Facoltativo) Fare clic sull'icona **Chiave di licenza** () e specificare la chiave di licenza da utilizzare per attivare il sistema operativo dopo l'installazione.
   e. Selezionare la posizione di storage preferita in cui si desidera distribuire l'immagine del sistema operativo dalla colonna **Storage**.

      Nota: per verificare che le distribuzioni del sistema operativo vengano completate correttamente, rimuovere tutto lo storage dal server gestito ad eccezione dello storage scelto per la distribuzione del sistema operativo.
   f. Verificare che lo stato di distribuzione per il server selezionato sia **Pronto**.
3. Selezionare tutti i server di destinazione e fare clic sull'icona **Distribuisci immagine** () per avviare la distribuzione del sistema operativo.
4. Nella scheda **Impostazioni personalizzate**, fare clic sulla scheda secondaria **Impostazioni di configurazione e di installazione automatica** e selezionare il file di installazione automatica personalizzato (ad esempio, `Windows_locale_customUnattend.xml`).



5. (Facoltativo) Nella scheda **Dominio di Active Directory**, specificare le informazioni per unire un dominio di Active Directory nell'ambito della distribuzione dell'immagine di Windows (vedere Integrazione con Windows Active Directory).
6. Nella scheda **Riepilogo**, verificare le impostazioni.
7. Fare clic su **Distribuisci** per distribuire il sistema operativo.

   Viene visualizzata la finestra di dialogo di installazione di Windows in giapponese.

   Al termine dell'installazione, la pagina di login di Windows viene visualizzata anche in giapponese.


Administrator
パスワード
パスワードのリセット

Capitolo 16. Scenari end-to-end per configurare nuovi dispositivi

Utilizzare questi scenari end-to-end per descrivere come utilizzare facilmente Lenovo XClarity Administrator per configurare i nuovi dispositivi in modo uniforme e semplice da riprodurre.

Distribuzione di ESXi su un'unità disco fisso locale

Utilizzare queste procedure per la distribuzione di VMware ESXi 5.5 su un'unità disco fisso installata in locale su un Nodo di elaborazione Flex System x240. Illustra come imparare un pattern server da un server esistente, come modificare il pattern categoria delle impostazioni UEFI estesa per quel pattern server e come installare VMware ESXi.

VMware ESXi 5.5 richiede la configurazione dello spazio I/O mappato alla memoria (MMIO) nei 4 GB iniziali del sistema. A seconda della configurazione, alcuni sistemi tentano di utilizzare più di 4 GB di memoria. Ciò potrebbe causare un errore. Per risolvere il problema, è possibile aumentare il valore dell'opzione MM Config a 3 GB tramite Setup utility per ciascun server su cui si desidera installare VMware ESXi 5.5.

In alternativa distribuire un pattern server che contenga uno dei pattern categoria UEFI estesa predefiniti relativi alla virtualizzazione, che imposta l'opzione MM Config e disabilita l'allocazione PCI 64-Bit Resource.

Distribuzione di un pattern di virtualizzazione predefinito

Un pattern categoria definisce le impostazioni firmware specifiche che possono essere riutilizzate da più pattern server. Per distribuire un pattern di virtualizzazione predefinito, creare un pattern server, quindi applicare un pattern UEFI esteso predefinito sul pattern server creato. Questo pattern server può, quindi, essere applicato a più server dello stesso tipo, ad esempio il Nodo di elaborazione Flex System x240 o il Nodo di elaborazione Flex System x880 X6.

Informazioni su questa attività

Durante la creazione di un pattern server, è possibile scegliere di completare la configurazione da soli oppure di apprendere gli attributi del pattern da un server esistente già configurato. Quando si apprende un nuovo pattern da un server esistente, la maggior parte degli attributi del pattern è già definita.

Per ulteriori informazioni sui pattern server e categoria, vedere Utilizzo di pattern server.

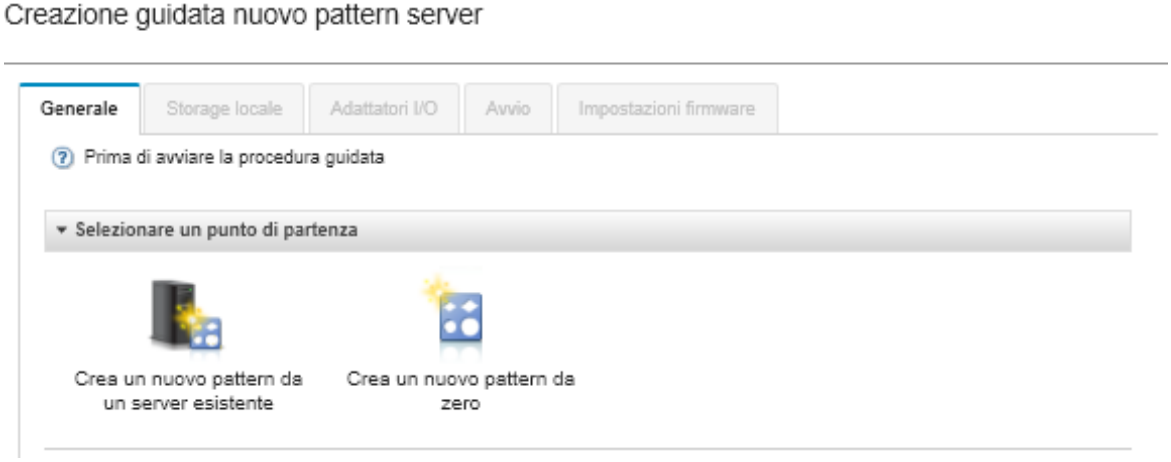
Procedura

Per apprendere un nuovo pattern da un server esistente, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Fare clic sulla scheda **Pattern server**.

Passo 3. Fare clic sull'icona **Crea** ( ). Viene visualizzata la finestra di dialogo Creazione guidata nuovi pattern server.



Passo 4. Fare clic su **Crea un nuovo pattern da un server esistente**. È possibile scegliere di creare un pattern da zero, tuttavia è molto più efficiente creare un pattern da un server esistente che dispone della configurazione desiderata.

Quando si crea un pattern server da un server esistente, XClarity Administrator apprende le impostazioni da un server gestito (tra cui le impostazioni BMC, l'UEFI e la porta estesa) e crea dinamicamente pattern categoria per tali impostazioni. Se il server è completamente nuovo, XClarity Administrator apprende le impostazioni di fabbrica. Se il server è in uso, XClarity Administrator apprende le impostazioni personalizzate. È possibile, quindi, modificare le impostazioni in maniera specifica per il server su cui si desidera distribuire questo pattern.

Passo 5. Selezionare il server da utilizzare come configurazione di base durante la creazione del pattern.

Nota: ricordare che il server scelto deve essere dello stesso modello dei server su cui si desidera distribuire il pattern server. Questo scenario è basato sulla scelta di un Nodo di elaborazione Flex System x240.

Passo 6. Immettere il nome del nuovo pattern e fornire una descrizione.

Ad esempio:

- Nome: **x240_ESXi_deployment**
- Descrizione: **Pattern con impostazioni UEFI estese appropriate per la distribuzione di VMware ESXi**

Passo 7. Fare clic su **Avanti** per caricare le informazioni dal server selezionato.

Passo 8. Nella scheda **Storage locale**, selezionare **Specifica configurazione storage** e scegliere uno dei tipi di storage. Quindi, fare clic su **Avanti**.

Per ulteriori informazioni sulle impostazioni dello storage locale, vedere Definizione di storage locale.

Passo 9. Nella scheda **Adattatori I/O**, immettere le informazioni sugli adattatori dei server su cui si desidera installare VMware ESXi.

Vengono visualizzati gli adattatori presenti nel server utilizzato come base.

Se tutti i Nodi di elaborazione Flex System x240 nell'installazione dispongono degli stessi adattatori, non è necessario modificare nessuna impostazione in questa scheda.

Per ulteriori informazioni sulle impostazioni degli adattatori I/O, vedere Definizione degli adattatori I/O.

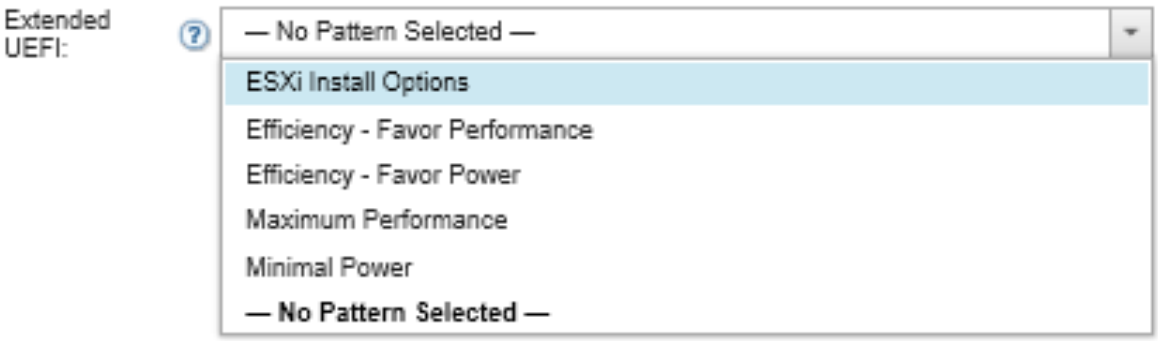
Passo 10. Fare clic su **Avanti** per continuare.

Passo 11. Nella scheda **Avvio**, configurare le impostazioni per l'ambiente di avvio solo legacy e gli ambienti di avvio SAN. A meno che non si stia utilizzando uno di questi ambienti, accettare l'impostazione predefinita **Avvio solo UEFI** e fare clic su **Avanti**.

Per ulteriori informazioni sulle impostazioni di avvio, vedere Definizione delle opzioni di avvio.

Passo 12. Nella scheda **Impostazioni firmware**, specificare il controller di gestione e le impostazioni del firmware UEFI da utilizzare per i server di destinazione quando questo pattern viene distribuito (selezionare, ad esempio, **Virtualizzazione x240**).

In questa scheda, è possibile scegliere uno dei pattern UEFI estesi predefiniti:



Per ulteriori informazioni sulle impostazioni del firmware, vedere Definizione delle impostazioni firmware.

Passo 13. Fare clic su **Salva e distribuisci** per salvare il pattern su XClarity Administrator e distribuirlo sui server su cui si desidera installare VMware ESXi.

Al termine

Dopo aver distribuito il pattern server su tutti i server, è possibile installare il sistema operativo su questi server.

Distribuzione di VMware ESXi su un Nodo di elaborazione Flex System x240

Utilizzare questa procedura come un flusso di esempio per illustrare il processo di distribuzione del sistema operativo ESXi su un Nodo di elaborazione Flex System x240.

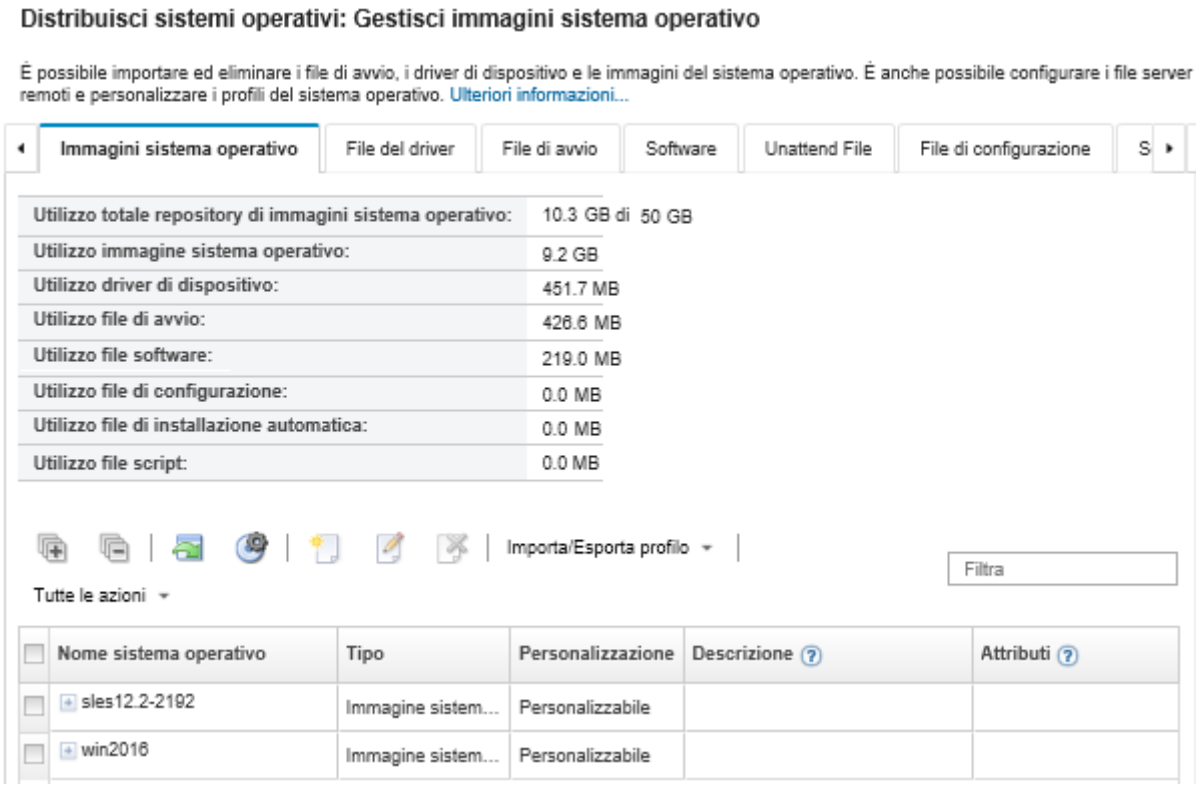
Prima di iniziare

Prima di iniziare questa procedura, verificare che Lenovo XClarity Administrator stia gestendo lo chassis in cui è installato il Nodo di elaborazione Flex System x240.

Procedura

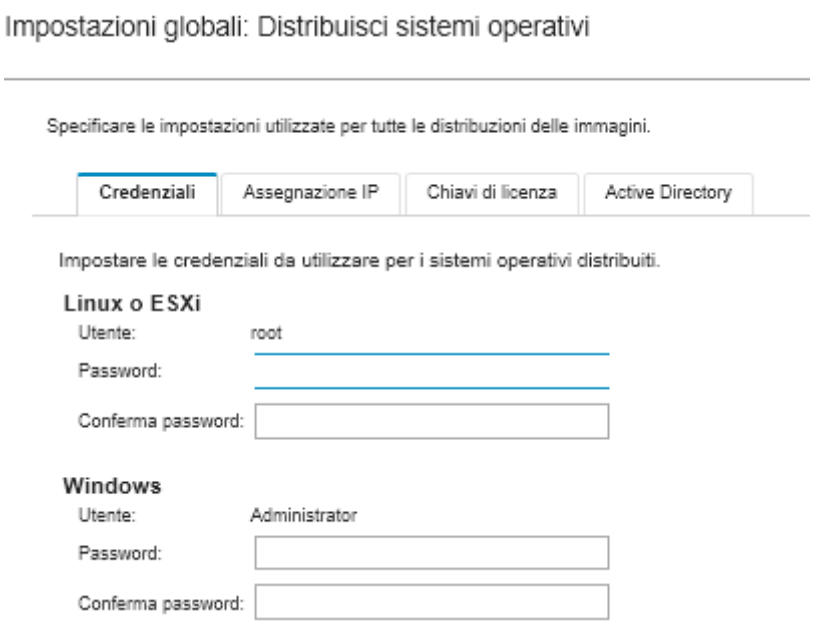
Completare le seguenti operazioni per distribuire il sistema operativo ESXi su un Nodo di elaborazione Flex System x240.

Passo 1. Verificare che l'immagine da distribuire sia già caricata nel repository di immagini del sistema operativo facendo clic su **Tutte le azioni → Gestisci immagini sistema operativo** per visualizzare un elenco di tutte le immagini disponibili.



Passo 2. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo**. Viene visualizzata la pagina Distribuisci immagini sistema operativo.

Passo 3. Configurare le impostazioni globali da utilizzate come impostazioni predefinite per tutte le distribuzioni delle immagini facendo clic su **Tutte le azioni → Impostazioni globali** per visualizzare la finestra di dialogo Impostazioni globali.



a. Sulla scheda **Credenziali**, immettere la password che deve essere utilizzata dall'account dell'amministratore per accedere al sistema operativo.

b. Sulla scheda **Assegnazione IP**, specificare in che modo l'indirizzo IP per il sistema operativo verrà assegnato al server.

   Se si sceglie l'opzione **Usa DHCP (Dynamic Host Configuration Protocol)** per assegnare gli indirizzi IP, le informazioni relative all'indirizzo IP non vengono visualizzate nella finestra di dialogo Modifica impostazioni di rete (vedere il Passo 8 9 a pagina 617). Se si sceglie l'opzione **Assegna indirizzo IP statico (IPv4)**, è possibile specificare un indirizzo IP, una sottorete e il gateway per ciascuna distribuzione.

c. Se desiderato, sulla scheda **Chiavi di licenza**, immettere una chiave di licenza di attivazione di massa.

d. Fare clic su **OK** per chiudere la finestra di dialogo.

Passo 4. Verificare che il server sia pronto per la distribuzione del sistema operativo selezionandolo. Inizialmente, è possibile che lo stato di distribuzione visualizzato sia Non pronto. Prima di poter distribuire un sistema operativo su un server, è necessario che lo stato di distribuzione sia Pronto.

Suggerimento: se si desidera distribuire lo stesso sistema operativo su tutti i server, è possibile scegliere più server in chassis di Flex System differenti. Il numero massimo dei server che è possibile scegliere è 28.

Passo 5. Fare clic nella colonna **Immagine da distribuire** e selezionare VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**).

Passo 6. Nella stessa colonna, fare clic sull'icona **Chiave di licenza** ( ) per immettere la chiave di licenza per questa distribuzione.

Suggerimento: è inoltre possibile scegliere di utilizzare la chiave di attivazione di massa immessa nella finestra di dialogo Impostazioni globali.

Passo 7. Verificare che l'opzione **Disco locale** sia selezionata nella colonna Storage.

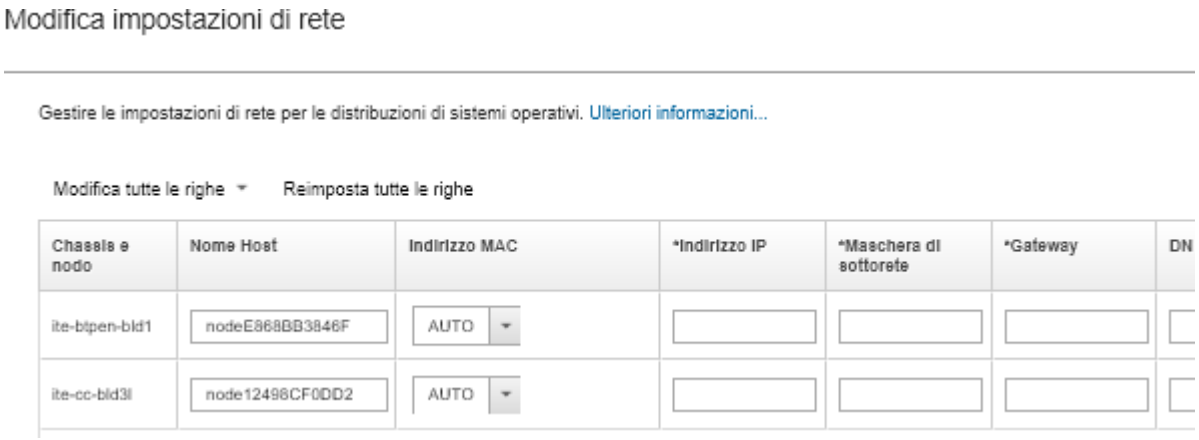
Passo 8. Fare clic su **Modifica** nella colonna **Impostazioni di rete** della riga del server per configurare le impostazioni di rete da utilizzare per questa distribuzione. Viene visualizzata la pagina Modifica impostazioni di rete.

Compilare i seguenti campi:

- Nome host
- Indirizzo MAC della porta sull'host in cui deve essere installato il sistema operativo
- Server DNS (Domain Name System), se richiesti
- Velocità MTU (Maximum Transmission Unit)

Nota: se si sceglie l'opzione **Assegna indirizzo IP statico (IPv4)** dalla finestra di dialogo Impostazioni globali (vedere Passo 3 4 a pagina 616) e immettere le seguenti informazioni:

- Indirizzo IPv4
- Subnet mask
- Gateway



Passo 9. Fare clic su **OK** per chiudere la finestra di dialogo.

Dalla pagina Distribuisci immagini sistema operativo verificare che il server mostri lo stato di distribuzione Pronto.

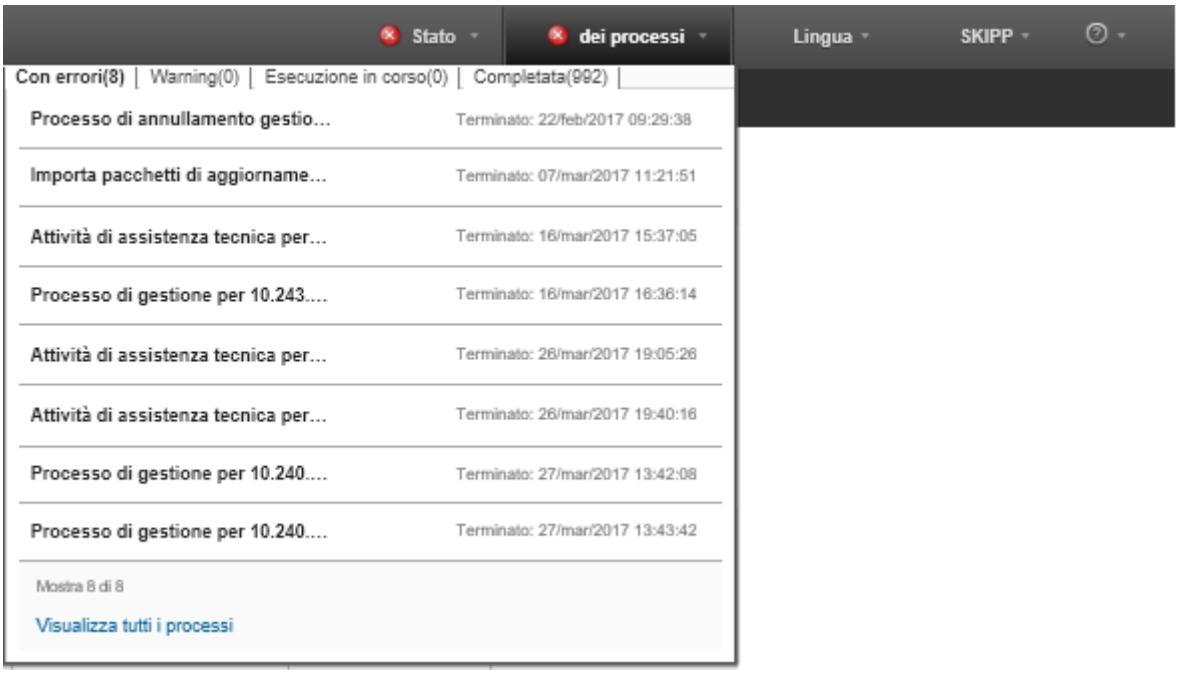
Passo 10. Distribuire il sistema operativo facendo clic su **Tutte le azioni → Distribuisci immagini**.

Passo 11. Dalla pagina di conferma, fare clic su **Distribuisci** per distribuire l'immagine.

Se nel server è installato un sistema operativo, verrà visualizzato un avviso in cui viene specificato che la distribuzione dell'immagine sovrascriverà il sistema operativo corrente.

Suggerimento: è possibile configurare una sessione di controllo remoto per visualizzare l'avanzamento dell'installazione. Fare clic su **Tutte le azioni → Controllo remoto** per avviare una sessione di controllo remoto con il server.

Quando viene distribuito il sistema operativo, Lenovo XClarity Administrator avvia un processo di tracciamento della distribuzione. Per visualizzare lo stato del processo di distribuzione, fare clic su **Processi** dalla barra dei menu di Lenovo XClarity Administrator. Quindi, fare clic sulla scheda **Esecuzione in corso**.

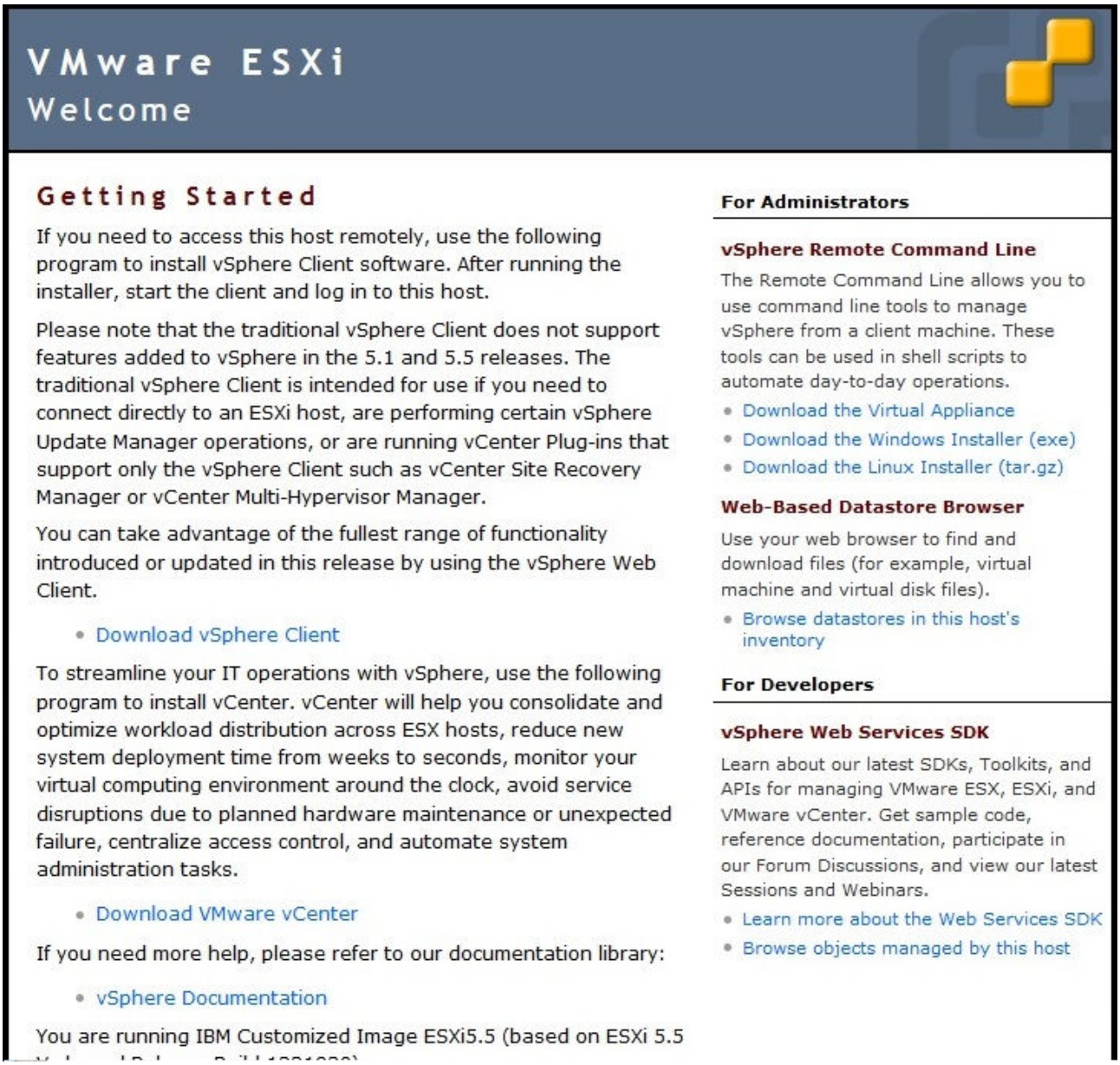


Passare il mouse sul processo in esecuzione per visualizzare i dettagli, ad esempio la percentuale del processo completata.

Risultati

Al termine della distribuzione del sistema operativo, accedere all'indirizzo IP specificato nella pagina Modifica impostazioni di rete per continuare il processo di configurazione.

Nota: La licenza fornita con l'immagine è una versione di prova gratuita di 60 giorni. L'utente sarà responsabile della soddisfazione di tutti i requisiti di licenza VMware.



Distribuzione di ESXi su storage SAN

Utilizzare queste procedure per la distribuzione VMware ESXi 5.5 su volumi SAN collegati ai server.

Quando si distribuisce un sistema operativo su una rete SAN, il sistema operativo viene distribuito sulla prima destinazione di avvio SAN che è configurata tramite un pattern server. Inoltre, un'unità disco fisso locale non può essere abilitata nel server che verrà avviato dalla rete SAN. Deve essere disabilitata o rimossa se è presente un'unità disco fisso.

Distribuzione di un pattern server per il supporto dell'avvio SAN

Quando si crea e si distribuisce un pattern server per il supporto dell'avvio di un sistema da rete SAN, verificare di aver identificato la destinazione di avvio SAN e gli adattatori che fanno parte del server.

Procedura

Per creare e distribuire un pattern server che supporti la distribuzione del sistema operativo su storage SAN, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Pattern**. Viene visualizzata la pagina Pattern di configurazione: pattern.

Passo 2. Per identificare gli ID WWPN e LUN dei volumi di storage in cui deve essere distribuito il sistema operativo, creare un pattern categoria.

a. Fare clic sulla scheda **Pattern categoria**.

b. Fare clic su **Pattern di destinazione avvio Fibre Channel**, quindi sull'icona **Crea** ( ).

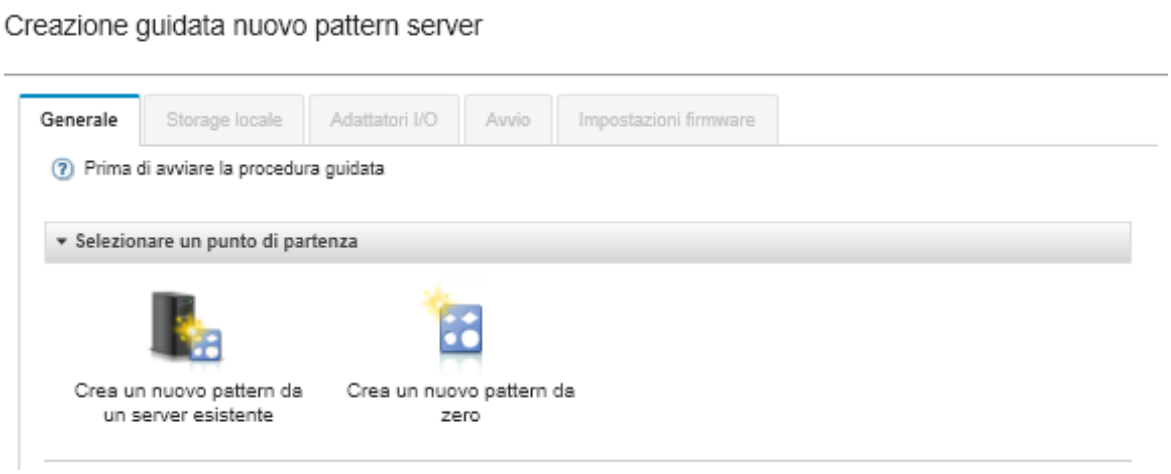
c. Immettere il WWPN della destinazione di storage.

Nota: fare clic su **Consenti più identificativi LUN** per assegnare identificativi LUN a più destinazioni agli stessi volumi di storage.

d. Fare clic su **Crea** per creare il pattern. La destinazione viene visualizzata nell'elenco dei pattern della destinazione di avvio Fibre Channel.

Passo 3. Fare clic sulla scheda **Pattern server** per creare un pattern.

Passo 4. Fare clic sull'icona **Crea** ( ). Viene visualizzata la finestra di dialogo Creazione guidata nuovi pattern server.



Passo 5. Fare clic su **Crea un nuovo pattern da zero**.

Passo 6. Nella scheda **Generale**:

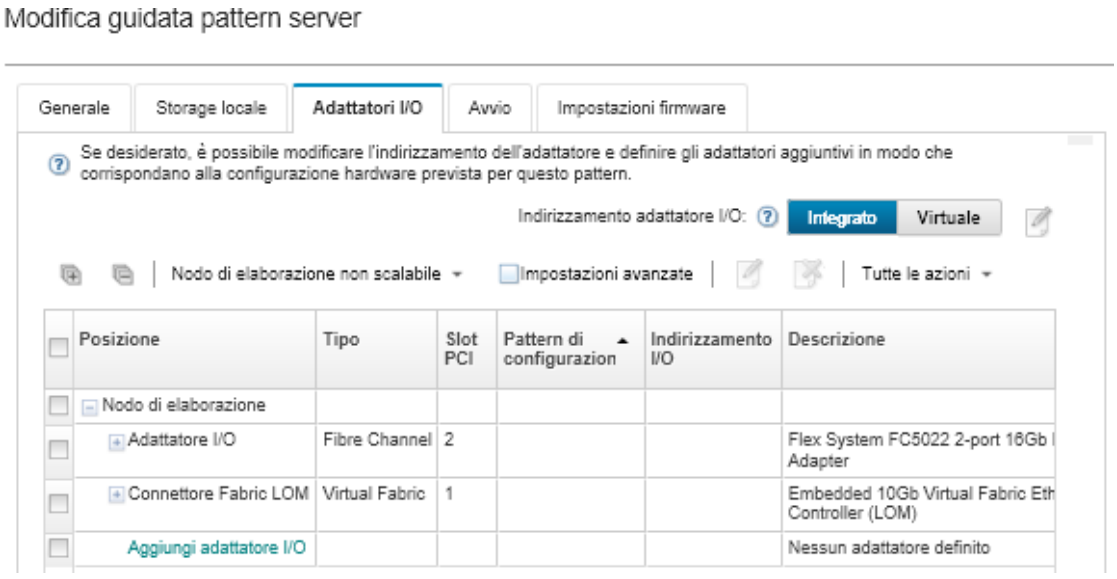
- Selezionare **Nodo di elaborazione Flex** per il fattore di forma.
- Specificare un nome (**x240_san_boot**) e una descrizione per il pattern.
- Fare clic su **Avanti**.

Passo 7. Per ottimizzare i tempi di avvio relativi alla scansione delle unità locali, nella scheda **Storage locale**, considerare la disabilitazione dell'adattatore dello storage locale se si utilizza un sistema senza disco. Quindi, fare clic su **Avanti**.

Passo 8. Nella scheda **Adattatori I/O**, aggiungere le schede Ethernet e Fibre Channel. Verificare che siano installate negli slot PCI appropriati.

a. Per ciascuna scheda, fare clic su **Aggiungi adattatore I/O**, scegliere lo slot PCI in cui è ubicata la scheda e selezionarla.

Nota: verificare di aver specificato una scheda Ethernet e una scheda Fibre Channel.



b. Verificare che l'indirizzamento dell'adattatore I/O sia impostato su **Virtuale**. Quindi, fare clic sull'icona **Modifica** per specificare la configurazione da utilizzare per l'indirizzamento virtuale Ethernet (MAC) e l'indirizzamento virtuale Fibre Channel (WWN).

Nota: dalla pagina Modifica indirizzamento virtuale, è possibile scegliere di utilizzare l'indirizzo MAC integrato per la scheda Ethernet disabilitando l'indirizzamento virtuale. Tuttavia, per selezionare e utilizzare il pattern della destinazione di avvio Fibre Channel, è necessario utilizzare l'indirizzamento virtuale per l'adattatore Fibre Channel.

c. Fare clic su **Avanti**.

Passo 9. Nella scheda **Avvio**, aggiungere il pattern della destinazione di avvio SAN creato in precedenza.

a. Nella scheda **Avvio SAN**, scegliere il pattern della destinazione di avvio definito.

b. Fare clic su **Avanti**.

Passo 10. Nella scheda **Impostazioni firmware**, definire tutti i pattern categoria aggiuntivi che devono essere inclusi in questo pattern server. È possibile definire i seguenti pattern categoria.

- **Informazioni sul sistema** (vedere Definizione delle impostazioni delle informazioni di sistema)
- **Interfaccia di gestione** (vedere Definizione delle impostazioni dell'interfaccia di gestione)
- **Dispositivo e porte I/O** (vedere Definizione delle impostazioni di dispositivi e porte I/O)
- **BMC estesa**. È possibile scegliere tra le impostazioni BMC apprese in precedenza (vedere Definizione delle impostazioni di controller di gestione esteso)
- **UEFI estesa**. È possibile scegliere tra le impostazioni predefinite o UEFI apprese in precedenza (vedere Definizione delle impostazioni UEFI estese)

Passo 11. Fare clic su **Salva e distribuisci** per salvare il pattern su Lenovo XClarity Administrator e distribuirlo sui server su cui si desidera installare VMware ESXi.

Al termine

Tenere in considerazione le seguenti operazioni dopo aver distribuito il pattern server su tutti i server.

1. Selezionare gli indirizzi WWPN virtualizzati creati e aggiungerli alla zona di storage in modo che il server possa raggiungere i LUN di storage specificati.

   Suggerimento: dopo aver distribuito il profilo del server, è possibile reperire gli indirizzi WWPN virtualizzati visualizzando il profilo del server.

   a. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Profili server**.

   b. Fare clic sul profilo del server distribuito (ad esempio, **x240_SAN_boot**). La scheda **Mapping indirizzi virtuali** visualizza l'elenco degli indirizzi.

2. Distribuire il sistema operativo sul server.

Distribuzione di VMware ESXi su storage SAN

Utilizzare questa procedura come flusso di esempio per illustrare il processo di distribuzione del sistema operativo ESXi sullo storage SAN collegato a un server.

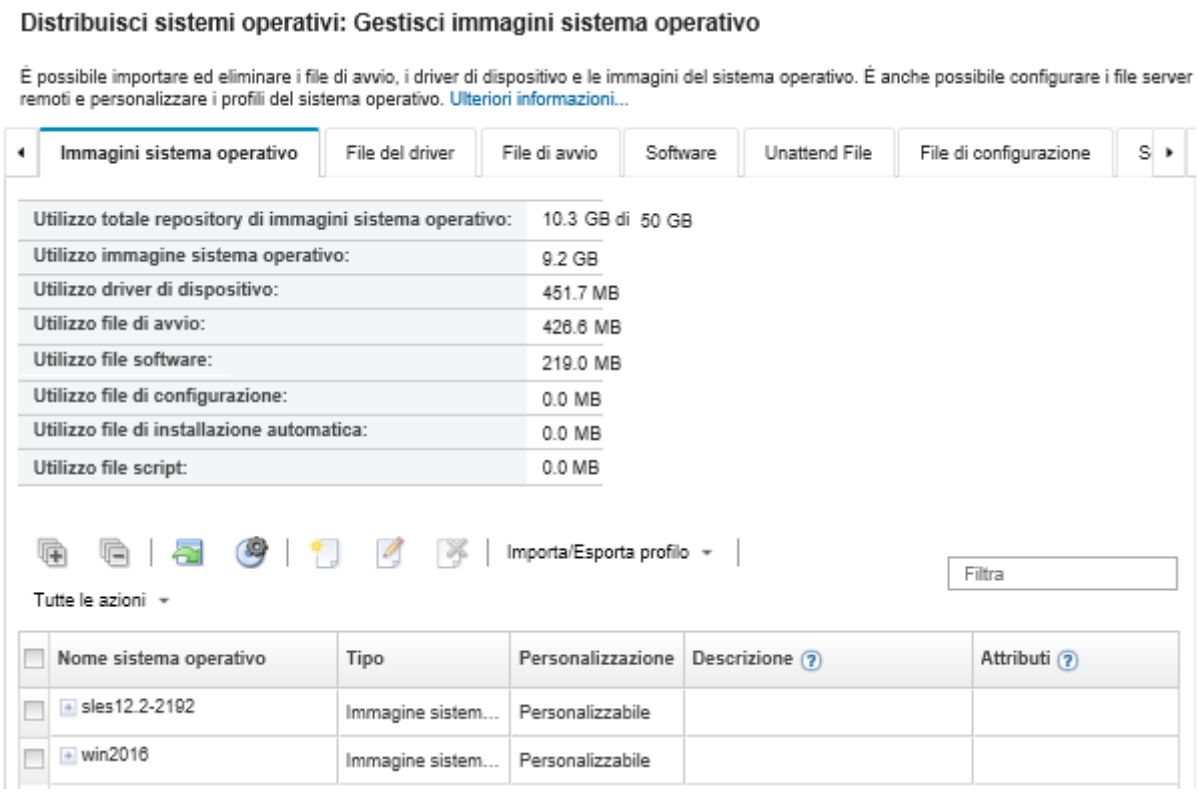
Prima di iniziare

Prima di iniziare questa procedura, verificare che Lenovo XClarity Administrator stia gestendo lo chassis in cui è installato il Nodo di elaborazione Flex System x220.

Procedura

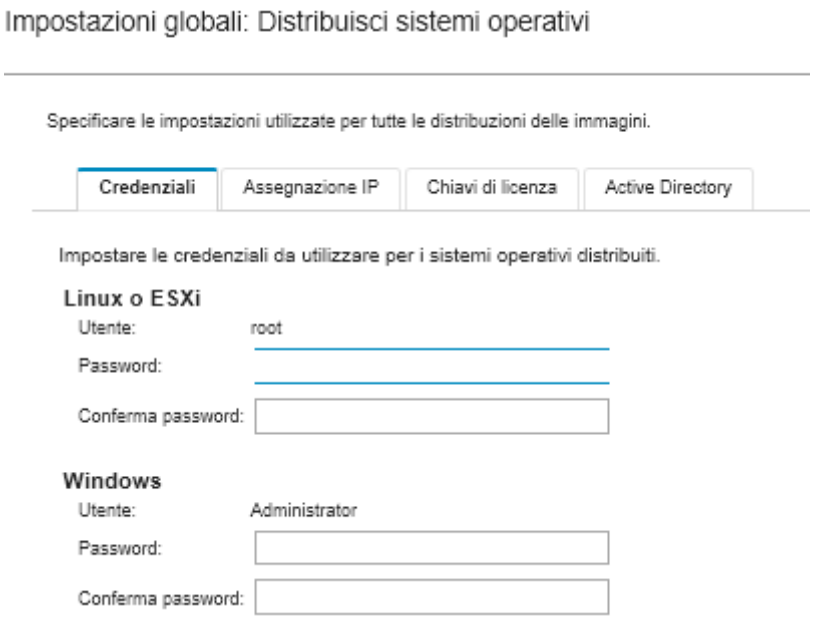
Per distribuire il sistema operativo ESXi su un Nodo di elaborazione Flex System x222, completare le seguenti operazioni.

Passo 1. Verificare che l'immagine da distribuire sia già caricata nel repository di immagini del sistema operativo facendo clic su **Tutte le azioni → Gestisci immagini sistema operativo**.



Passo 2. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Provisioning → Distribuisci immagini sistema operativo**

Passo 3. Configurare le impostazioni globali da utilizzate come impostazioni predefinite per tutte le distribuzioni delle immagini facendo clic su **Tutte le azioni → Impostazioni globali** per visualizzare la finestra di dialogo Impostazioni globali: distribuisci sistemi operativi.



a. Sulla scheda **Credenziali**, immettere la password che deve essere utilizzata dall'account dell'amministratore per accedere al sistema operativo.

b. Sulla scheda **Assegnazione** IP, specificare in che modo l'indirizzo IP per il sistema operativo deve essere assegnato al server.

   Se si sceglie l'opzione **Usa DHCP (Dynamic Host Configuration Protocol)** per assegnare gli indirizzi IP, le informazioni relative all'indirizzo IP non verranno visualizzate nella finestra di dialogo Modifica impostazioni di rete (vedere il Passo 8 9 a pagina 626). Se si sceglie l'opzione **Assegna indirizzo IP statico (IPv4)**, è possibile specificare un indirizzo IP, una sottorete e il gateway per ciascuna distribuzione.

c. Se desiderato, sulla scheda **Chiavi di licenza**, immettere una chiave di licenza di attivazione di massa.

d. Fare clic su **OK** per chiudere la finestra di dialogo.

Passo 4. Selezionare il server sul quale verrà eseguita la distribuzione del sistema operativo per verificare se sia pronto per l'operazione. Inizialmente, è possibile che lo stato di distribuzione visualizzato sia Non pronto. Prima di poter distribuire un sistema operativo su un server, lo stato di distribuzione deve essere Pronto.

Suggerimento: se si desidera distribuire lo stesso sistema operativo su tutti i server, è possibile scegliere più server da chassis di Flex System differenti. Il numero massimo dei server che è possibile scegliere è 28.

Passo 5. Fare clic nella colonna **Immagine da distribuire** e selezionare VMware ESXi 5.5 (**esxi5.5_2.33| esxi5.5_2.33-x86_64-install-Virtualization**).

Passo 6. Nella stessa colonna, fare clic sull'icona **Chiave di licenza** ( ) per immettere la chiave di licenza per questa distribuzione.

Suggerimento: è inoltre possibile scegliere di utilizzare una chiave di attivazione di massa immessa nella finestra di dialogo Impostazioni globali: distribuisci sistemi operativi.

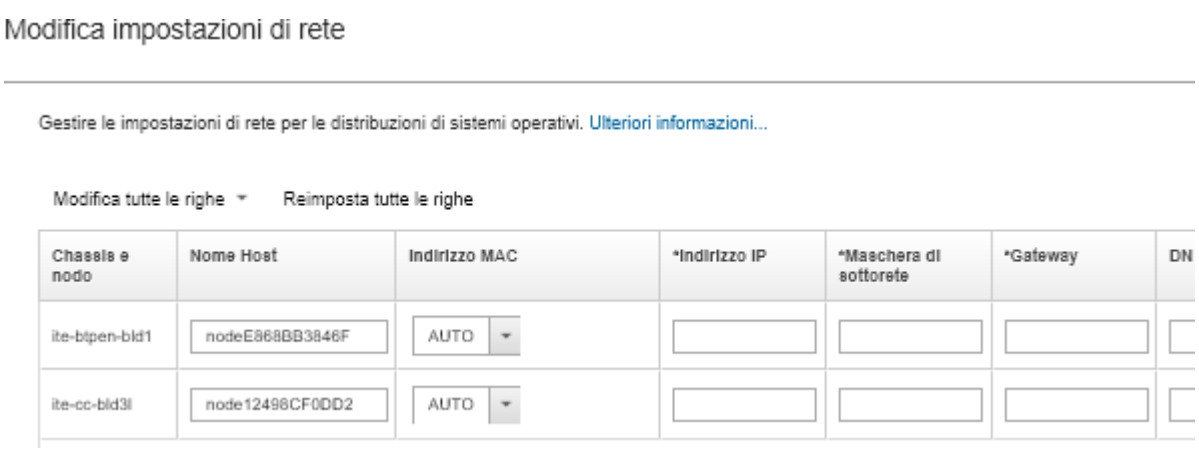
Passo 7. Nella colonna **Storage**, selezionare lo storage SAN su cui si desidera distribuire il sistema operativo.

Lo storage è così elencato:
`LUN: <LUN VALUE>  WWPN: <WWPN_VALUE>`

Passo 8. Fare clic su **Modifica** nella colonna **Impostazioni di rete** della riga del server per configurare le impostazioni di rete da utilizzare per questa distribuzione. Viene visualizzata la pagina Modifica impostazioni di rete.

Compilare i seguenti campi:
- Nome host
- Indirizzo MAC della porta sull'host in cui verrà installato il sistema operativo
- Server DNS (Domain Name System), se richiesti
- Velocità MTU (Maximum Transmission Unit)

Nota: se si sceglie **Assegna indirizzo IP statico (IPv4)** dalla finestra di dialogo Impostazioni globali: distribuisci sistemi operativi (Passo 3 4 a pagina 624), immettere, inoltre, le seguenti informazioni:
- Indirizzo IPv4
- Subnet mask
- Gateway



Passo 9. Fare clic su **OK** per chiudere la finestra di dialogo.

Nella pagina Distribuisci immagini sistema operativo, il server mostra l'impostazione "Pronto" relativamente allo stato di distribuzione.

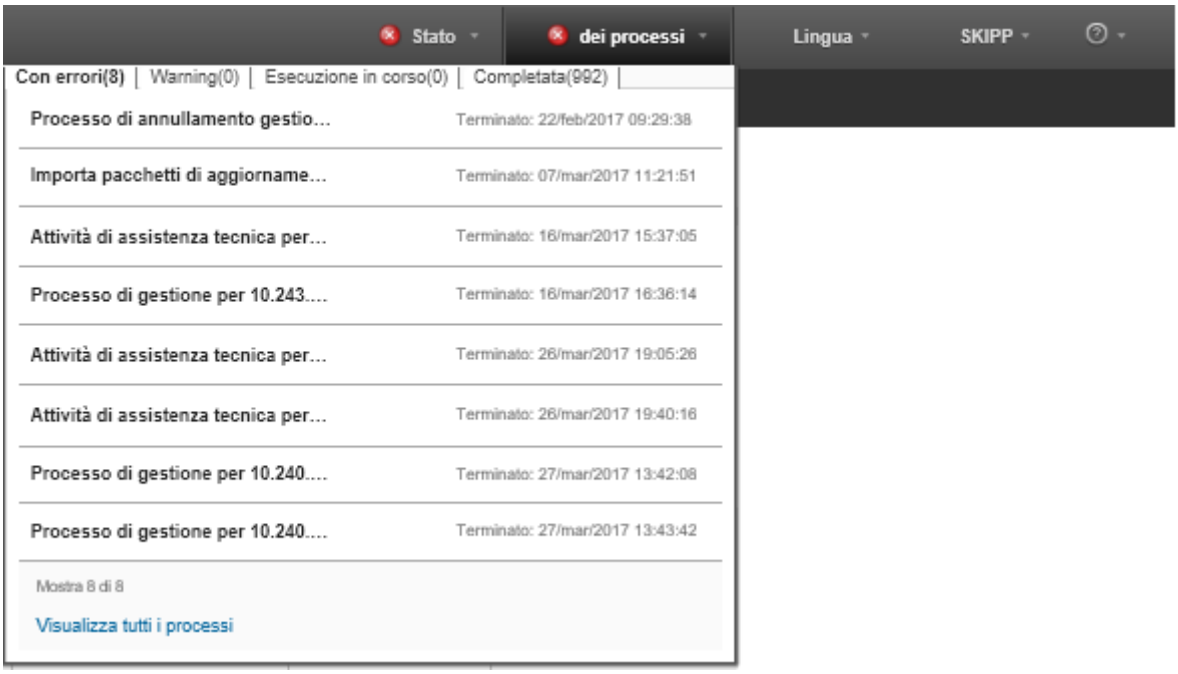
Passo 10. Distribuire il sistema operativo facendo clic su **Tutte le azioni → Distribuisci immagini**.

Passo 11. Dalla pagina di conferma, fare clic su **Distribuisci** per distribuire l'immagine.

Se nel server è attualmente installato un sistema operativo, verrà visualizzato un avviso in cui viene specificato che la distribuzione dell'immagine sovrascriverà il sistema operativo corrente.

Suggerimento: è possibile configurare una sessione di controllo remoto per visualizzare l'avanzamento dell'installazione. Fare clic su **Tutte le azioni → Controllo remoto** per avviare una sessione di controllo remoto con il server.

Quando viene distribuito il sistema operativo, Lenovo XClarity Administrator avvia un processo di tracciamento della distribuzione. Per visualizzare lo stato del processo di distribuzione, fare clic su **Processi** dalla barra dei menu di Lenovo XClarity Administrator. Quindi, fare clic sulla scheda **Esecuzione in corso**.

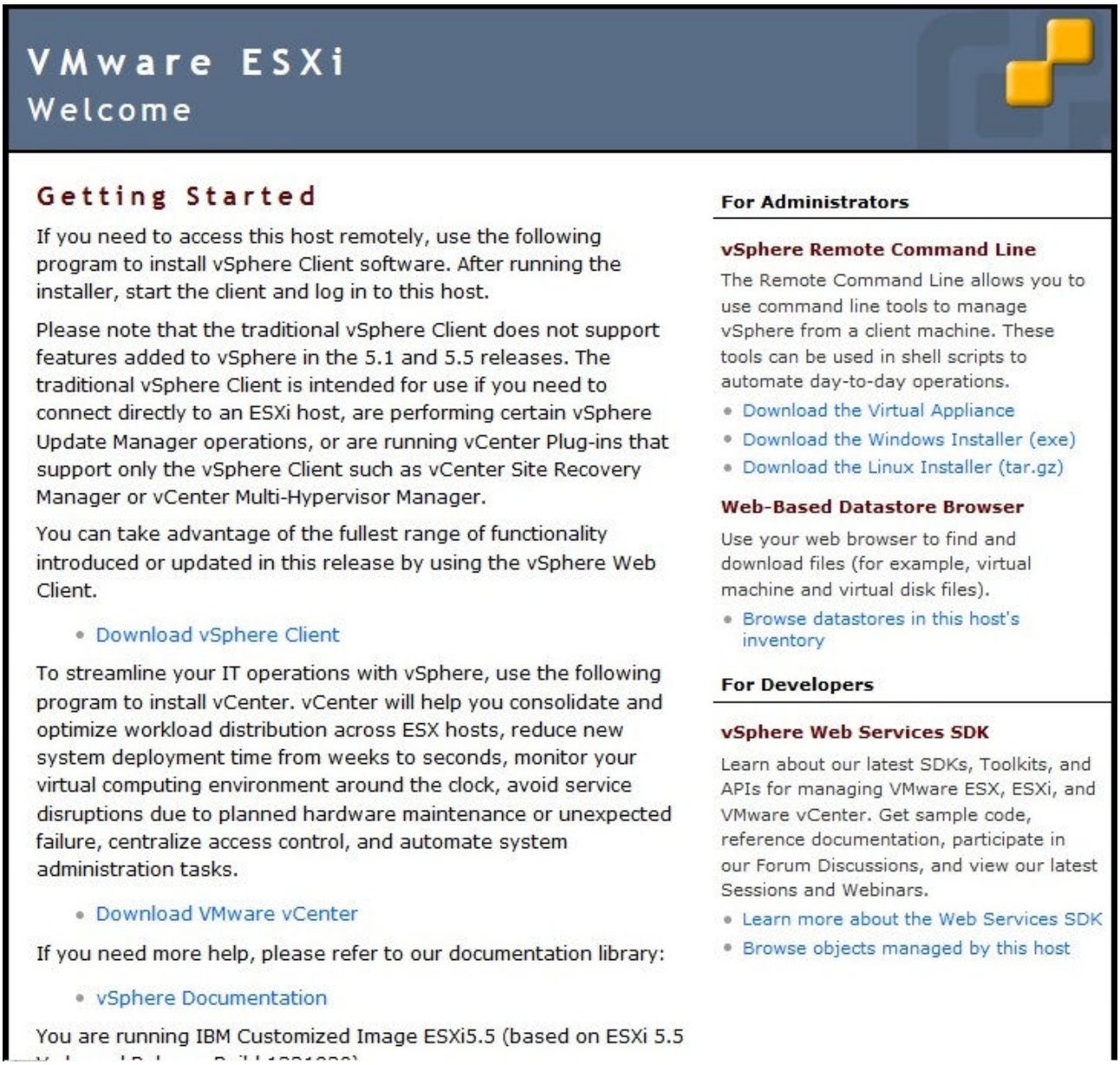


Passare il mouse sul processo in esecuzione per visualizzare i dettagli, ad esempio la percentuale del processo completata.

Risultati

Al termine della distribuzione del sistema operativo, accedere all'indirizzo IP specificato nella pagina Modifica impostazioni di rete per continuare il processo di configurazione.

Nota: La licenza fornita con l'immagine è una versione di prova gratuita di 60 giorni. L'utente sarà responsabile della soddisfazione di tutti i requisiti di licenza VMware.


VMware ESXi
Welcome
Getting Started
If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Please note that the traditional vSphere Client does not support features added to vSphere in the 5.1 and 5.5 releases. The traditional vSphere Client is intended for use if you need to connect directly to an ESXi host, are performing certain vSphere Update Manager operations, or are running vCenter Plug-ins that support only the vSphere Client such as vCenter Site Recovery Manager or vCenter Multi-Hypervisor Manager.
You can take advantage of the fullest range of functionality introduced or updated in this release by using the vSphere Web Client.
Download vSphere Client
To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.
Download VMware vCenter
If you need more help, please refer to our documentation library:
vSphere Documentation
You are running IBM Customized Image ESXi5.5 (based on ESXi 5.5
For Administrators
vSphere Remote Command Line
The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.
Download the Virtual Appliance
Download the Windows Installer (exe)
Download the Linux Installer (tar.gz)
Web-Based Datastore Browser
Use your web browser to find and download files (for example, virtual machine and virtual disk files).
Browse datastores in this host's inventory
For Developers
vSphere Web Services SDK
Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.
Learn more about the Web Services SDK
Browse objects managed by this host

Informazioni particolari

I riferimenti contenuti in questa pubblicazione relativi a prodotti, servizi o funzioni Lenovo non implicano che la Lenovo intenda renderli disponibili in tutti i paesi in cui opera. Consultare il proprio rappresentante Lenovo locale per in formazioni sui prodotti e servizi disponibili nel proprio paese.

Qualsiasi riferimento a un prodotto, programma o servizio Lenovo non implica che debba essere utilizzato esclusivamente quel prodotto, programma o servizio Lenovo. Qualsiasi prodotto, programma o servizio funzionalmente equivalente che non violi alcun diritto di proprietà intellettuale Lenovo può essere utilizzato. È comunque responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri prodotti, programmi o servizi.

Lenovo può avere applicazioni di brevetti o brevetti in corso relativi all'argomento descritto in questo documento. La distribuzione del presente documento non concede né conferisce alcuna licenza in virtù di alcun brevetto o domanda di brevetto. Per ricevere informazioni, è possibile inviare una richiesta scritta a:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO FORNISCE QUESTA PUBBLICAZIONE "COSÌ COM'È" SENZA ALCUN TIPO DI GARANZIA, SIA ESPRESSA SIA IMPLICITA, INCLUSE, MA NON LIMITATE, LE GARANZIE IMPLICITE DI NON VIOLAZIONE, COMMERCIABILITÀ O IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcune giurisdizioni non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni, quindi la presente dichiarazione potrebbe non essere applicabile all'utente.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le modifiche alle presenti informazioni vengono effettuate periodicamente; tali modifiche saranno incorporate nelle nuove pubblicazioni della pubblicazione. Lenovo si riserva il diritto di apportare miglioramenti e modifiche al prodotto o al programma descritto nel manuale in qualsiasi momento e senza preavviso.

I prodotti descritti in questa documentazione non sono destinati all'utilizzo di applicazioni che potrebbero causare danni a persone. Le informazioni contenute in questa documentazione non influiscono o modificano le specifiche o le garanzie dei prodotti Lenovo. Nessuna parte di questa documentazione rappresenta l'espressione o una licenza implicita fornita nel rispetto dei diritti di proprietà intellettuale di Lenovo o di terze parti. Tutte le informazioni in essa contenute sono state ottenute in ambienti specifici e vengono presentate come illustrazioni. Quindi, è possibile che il risultato ottenuto in altri ambienti operativi varii.

Lenovo può utilizzare o distribuire le informazioni fornite dagli utenti secondo le modalità ritenute appropriate, senza incorrere in alcuna obbligazione nei loro confronti.

Tutti i riferimenti ai siti Web non Lenovo contenuti in questa pubblicazione sono forniti per consultazione; per essi Lenovo non fornisce alcuna approvazione. I materiali reperibili presso questi siti non fanno parte del materiale relativo al prodotto Lenovo. L'utilizzo di questi siti Web è a discrezione dell'utente.

Qualsiasi dato sulle prestazioni qui contenuto è stato determinato in un ambiente controllato. Quindi, è possibile che il risultato ottenuto in altri ambienti operativi varii significativamente. Alcune misurazioni possono essere state effettuate sul sistemi a livello di sviluppo e non vi è alcuna garanzia che tali misurazioni resteranno invariate sui sistemi generalmente disponibili. Inoltre, alcune misurazioni possono essere state stimate mediante estrapolazione. I risultati reali possono variare. Gli utenti di questo documento dovrebbero verificare i dati applicabili per il proprio ambiente specifico.

Marchi

LENOVO, SYSTEM, NEXTSCALE, SYSTEM X, THINKSERVER, THINKSYSTEM e XCLARITY sono marchi di Lenovo.

Intel è un marchio di Intel Corporation negli Stati Uniti e/o in altri paesi.

Linux è un marchio registrato di Linus Torvalds.

Microsoft, Windows, Windows Server, Windows PowerShell, Hyper-V, Internet Explorer e Active Directory sono marchi registrati del gruppo di società Microsoft.

Mozilla e Firefox sono marchi registrati di Sun Microsystems, Inc. negli Stati Uniti e/o in altri paesi.

Nutanix è un marchio e brand di Nutanix, Inc. negli Stati Uniti e/o in altri paesi.

Red Hat è un marchio registrato di Red Hat, Inc. negli Stati Uniti e in altri paesi.

SUSE è un marchio di SUSE IP Development Limited o delle relative filiali e consociate.

VMware vSphere è un marchio registrato di VMware negli Stati Uniti e/o in altri paesi.

Tutti gli altri marchi sono di proprietà dei rispettivi titolari.

Lenovo